Vol. 666 31 December Desember 2020 No. 44048

PART 1 OF 3

For purposes of reference, all Proclamations, Government Notices, General Notices and Board Notices published are included in the following table of contents which thus forms a weekly index. Let yourself be guided by the gazette numbers in the righthand column:

Weekly Index

Alle Proklamasies, Goewermentskennisgewings, Algemene Kennisgewings en Raadskennisgewings gepubliseer, word vir verwysingsdoeleindes in die volgende Inhoudopgawe ingesluit wat dus weeklikse indeks voorstel. Laat uself deur die Koerantnommers in die regterhandse kolom lei:

Weeklikse Indeks

Contents

GOVERNMENT NOTICES • GOEWERMENTSKENNISGEWINGS

DEPARTMENT OF HOME AFFAIRS

NO. 1425 31 DECEMBER 2020

Draft OIDM policy: Public Consultation
Version of 22 December 2020

home affairs
Department:
Home Affairs
REPUBLIC OF SOUTH AFRICA

DRAFT OFFICIAL IDENTITY MANAGEMENT POLICY

PUBLIC CONSULTATION VERSION

22 DECEMBER 2020

TABLE OF CONTENTS

GLOSSARY

Assigned sex: the sex category assigned to an individual by medical, legal, or other social authorities. Assigned sex is often determined to be either male or female based solely on a child's genitalia at birth, and it may not align with gender identity.

Biometric (biometric data): measurable biological or behavioural characteristic of a natural person that can be used to determine or to verify their identity; e.g. face, fingerprints and voice.

Biometric verification: automated verification of a person based on their biological and behavioural characteristics, e.g. the facial matching conducted by the FVS.

Civil registration: continuous/permanent, compulsory, universal recording of the occurrence and characteristics of vital events that could affect the legal status of individuals in a population such as birth, marriage or death. This means the State must record all the events in an individual's life, in line with decrees, regulations or laws of the country and fully respecting rules regulating the protection and privacy of individual information.

Consent: expressed or implied specific and informed permission given voluntarily by an individual with the capacity to understand their decision to offer the permission.

Credential: technology used to authenticate a user's identity (also referred to as an authentication credential). The user possesses the credential and controls its use through authentication protocols. A credential may be a username and password, cryptographic key or other form of secret used to verify a user's digital identity. To use a digital identity in requesting access to a resource, a subject presents an authentication credential. The credentials, once authenticated, are taken as proof that the subject owns the claimed digital identity, and that the subject is permitted to access the resources/services which are associated with their digital identity.

Data dump: transfer of a large amount of data between two systems, often over a network connection. For example, a database can be dumped to another network server, where it could be used by other software applications or analysed by a person.

Digital identity: a person's set of attributes that uniquely describes the person engaged in an online transaction under the identity ecosystem.

Gender: socially constructed roles, behaviours, and personal characteristics that a given society considers appropriate for men, women, and others. People whose gender is neither man nor woman may describe themselves as being in an intermediate state between man and woman, being both man and woman, being neither or belonging to another gender altogether.

Gender identity: an individual's deeply-rooted internal sense of gender. This resource uses the term "trans" to include a diverse range of people whose gender identity is different from the sex they were assigned at birth.

Identity: a person's set of attributes that uniquely describes the person within a given context.

Identity attribute: a piece of information relating to identity (e.g. full name or date of birth).

Identity theft: the deliberate use of the identity of another living or deceased person.

Intersex: an adjective referring to a person whose sexual anatomy, reproductive organs and/or chromosome patterns do not fit the typical definition of male or female. These anatomical differences are often perceived to be both male and female at the same time; not quite male or female; or neither male or female. These congenital differences in anatomical sex often result in physical differences in secondary sex characteristics such as muscle mass, hair distribution, breast development and stature.

Non-binary person: non-binary or genderqueer is a spectrum of gender identities that are not exclusively masculine or feminine – identities that are outside the gender binary (male and female). Non-binary identities can fall under the transgender umbrella, since many non-binary people identify with a gender that is different from their assigned sex.

Official identity: personal information including biometric data that is collected and stored by the DHA according to the established legislation.

Sex: a classification of people as male, female, indeterminate sex or intersex. Most individuals are assigned a sex at birth based on a combination of bodily characteristics such as genitals and internal reproductive organs, and less frequently based on their chromosomes.

Transgender: an adjective referring to a person whose gender identity or expression is different from their assigned sex.

Transition: the process that a trans person undergoes to live in their gender identity. It may include social gender recognition (e.g. changing one's appearance), legal gender recognition (e.g. changing one's name and sex / gender details on documents) and/or medical transition (e.g. hormones or surgeries that result in physical changes to a trans person's body).

Validation (in an identity proofing context): a check that the attribute exists and is under the control of the individual (e.g. SMS activation code being sent to a mobile phone number to confirm control of the associated phone number).

Validation (in an integration testing context): testing a system under controlled conditions providing evidence that the system satisfies trust framework requirements and satisfies the intended use and user needs. Validation involves testing that functionality works as specified, designed and constructed, including intentionally making things go wrong when they should not and things happen when they should not (testing boundary conditions) to ensure that the system is robust when in production.

Verification (in an integration testing context): provides confirmation, using objective evidence, that trust framework requirements have been fulfilled. Verification involves evaluating whether a system complies with a regulation, requirement, specification, or imposed condition.

ABBREVIATIONS

4IR	Fourth industrial revolution
Abis	Automated Biometric Identification System
AU	African Union
DHA	Department of Home Affairs
EMCS	Enhanced Movement Control System
Hanis	Home Affairs National Identity System
ICAO	International Civil Aviation Organization
ID	Identity document
MCS	Movement Control System
NIIS	National Immigration Information System
NIS	National Identity System
NPR	National Population Register
POPI	The Protection of Personal Information Act 4 of 2013

SECTION A: BACKGROUND, ANALYSIS AND CONTEXT

Chapter 1: The Department of Home Affairs mandate

1.1 Overview of the DHA mandate

The Department of Home Affairs (DHA) mandate straddles a number of essential elements of all South Africans' lives, including activities carried out by the private sector. The DHA is the sole authority and has a leadership role in South Africa on identity, identity management and identity management systems across government and economic spheres.

The DHA's sole mandate includes the sole authority to affirm and regulate official identity and South African citizenship. To fully appreciate the DHA's mandate, the Constitution of the Republic of South Africa is the first and primary point of reference. The Constitution's provisions are accompanied by the concepts of sovereignty, identity, citizenship, national security interests and actively enabling citizen empowerment and economic development. In promoting and fulfilling the Constitution's provisions, the DHA is mandated to develop and manage an identification system. According to the Constitution, no citizen may be deprived of citizenship (Section 20), every child has the right to a name and a nationality from birth (Section 28(1)(a)), everyone has the right to leave the Republic (Section 21(2)), and every citizen has the right to a passport (Section 21(4)). Also of direct relevance is a just and efficient administration as defined in Chapter 10 of the Constitution.

The mandate and strategic relevance of the DHA is expressed in the *White Paper on Home Affairs* (the White Paper) as follows:

- Mandate one: Management of citizenship and civil registration
- Mandate two: Management of international migration
- Mandate three: Management of refugee protection

The DHA has a sole mandate over its services, unlike other government departments such as Health and Education whose services can be privatised. Only the DHA can affirm a person's identity, issue a South African identity document or passport and register a birth, a death or a marriage. No other department can affirm or grant citizenship. Only the DHA has the authority to allow anyone to enter or leave South Africa, and to issue a permit and a visa. Only the DHA can grant asylum seeker or refugee status.

The overarching importance of identity and identity management is evident and clear in this mandate. As observed in the White Paper, managing identity and the status of legal

persons in a society, particularly in a modern society, continues to be essential for societies to organise work, distribute resources and ensure that people's rights and identities are protected. And where those looking for economic opportunities and those who claim asylum create a movement of people, managing migration means minimising risks while maximising the benefits of migration in terms of knowledge, productivity and trade.

In realising the goals of the mandate, the DHA is structured around two pillars of its programmes and work. The first is the programme on citizen affairs, which covers the activities of the Civic Affairs branch at national and provincial levels. This involves providing and managing the identity and status services for citizens, permanent residents and persons accorded refugee status. The second is the programme on immigration affairs, which is responsible for implementing immigration legislation, managing the immigration system, functions at ports of entry, the immigration inspectorate and deportations, the visa and permitting regime, and processing asylum seekers and refugees.

1.2 DHA as a custodian of identity management in South Africa

The policy framework and laws that enable the State to establish the legal status of every individual in South Africa is the foundation of our sovereignty and the legitimate exercise of State power. Affirming the identity and status of every citizen at birth is indispensable for the State, which must respect, protect, promote and fulfil their constitutional rights.

The third clause of the founding provisions in Chapter 1 of the Constitution states, "National legislation must provide for the acquisition, loss and restoration of citizenship". Without a national register of citizens, this obligation cannot be fulfilled and there cannot be "Universal adult suffrage and a national common voter's roll..." as prescribed in the first clause.

The very notion of sovereignty and the legal status, integrity and security of the South African State, South Africans and all members of society rest, to a large extent, on the information and functions that are within the legal jurisdiction of the DHA. This is a reference to identity as a legally established concept composed of specified information.

The DHA's core functions are a fundamental part of all human societies. Throughout history, managing identity and status has been essential for societies to organise work, distribute resources and ensure that people's rights and identities are protected.

Identity refers to the unique set of identifiers that distinguishes an individual from all other individuals. In modern states the key identifier is typically a unique number allocated soon after birth, and can be linked to that person by biometrics and other means.

Status is the assigned category of persons based on shared criteria, such as being citizens of a country, married, a child, a voter or a mother. Civic status refers to criteria attributed to citizens by a state, typically including a record of vital life events such as marriage.

The DHA plays a central role in both the State and society though its mandate, responsibilities and functions as stipulated in various Acts including the Identification Act 68 of 1997.

The Identification Act makes provision for compiling and maintaining the population register for the population of the Republic. It also provides for issuing identity documents to persons (citizens and permanent residents) whose particulars are included in the population register. In 1982, the DHA established the national population register (NPR) to enable it to store biometric data (fingerprints and face image) and other data specified in the Act. This register can be used to determine a person's identity, linked to the biographical information and personal information for civil registrations, and compile and store particulars as stipulated in the Identification Act. However, as the NPR is outdated and only data stores are limited to citizens and permanent residents, it will be replaced by an inclusive and secure National Identity System (NIS). The NIS will store the particulars of all persons, citizens and non-citizens who are within the territorial jurisdiction of the country. The NIS will be the backbone of identity management and cut across the social, political and economic spheres.

The DHA is the established legal institution within the South African government mandated to carry out the responsibility for identity management. The identity management policy establishes the vision, goals and objectives, as well as the approach that the DHA adopts towards establishing a modern and secure NIS. The NIS will become the backbone for systems, networks and platforms to facilitate providing goods and services to citizens and other legal persons, in the government-wide consolidation of processes and systems to enhance national security and in the contribution to economic development and growth.

Accurate and reliable data and information on all South Africans such as birth, marriage, death records and other vital statistics is a necessity for planning and formulating appropriate policy and programme responses to cater for the needs of South Africans. All these are essential services offered by the DHA. The policy on identity management is anchored in the DHA's crucial role as part of this critical function, as demonstrated when the State provides socio-economic goods and services such as non-contributory social assistance, housing, education and healthcare services to its citizens and other legally

prescribed persons. In addition, for the economy to function to its full potential, identity management is used in various forms through multiple channels, technologies and innovations by the private sector and its markets in financial services and transactions.

Identity management, under the DHA's legal mandate as the sole provider of official identity and civic status verification in South Africa, is an important and pressing issue given the technological advances unfolding globally, especially the growth of the digital economy. Innovations and new technologies are sweeping the globe at rapid pace, including here in South Africa, and are rapidly disrupting and changing the way we all behave, live and work. This phenomenon has been dubbed the fourth industrial revolution (4IR), also known as the digital revolution, and marks a major turning point in our collective local and global development.[1]

Identity management in its multiple forms is an integral part of this era of 4IR, the digital economy, e-identity, national security, global threats, and the use of technology by governments to improve the quality of life of citizens. The ever-changing, technology-driven context and environment is accompanied by demands from stakeholders within and outside government, with economic activity demanding digital automation.

The 4IR has implications for South Africa in identity management, digital identity development, cybersecurity, the digital economy and other new technology-driven frontiers. South Africa's sixth administration saw the former Department of Communications, Telecommunications and Postal Services becoming the Department of Communications and Digital Technologies[2], with a context-relevant mandate. This indicates an awareness of the pressure exerted by an external national and global environment that is adopting new digital technologies to which governments have to respond. For these reasons, the DHA is building an NIS that is inclusive, digital, secure, accurate, confidential and responsive.

---

1 Project iKUSASA: A Digital Roadmap to a Modernised, Future-fit DHA. In this document, the DHA of the future is described as 'a digitally-led organisation that is responsive to the changing needs of South Africa's citizens and other stakeholders as well as the opportunities that digital thinking provides to promote value-for-money service delivery.'

2 In South Africa the raising, at the national level, of digital technologies to the political and policy levels demonstrates the emerging appreciation by the sixth administration of the pervasive impact changes in this area will have on South Africa and its systems in government and the private sector.

Chapter 2: Problem analysis and rationale for the identity management policy

2.1 Problem analysis

The Identification Act is now more than 20 years old. It is not based on a policy that considers key local and global developments in managing official personal information. This in part explains why the current legislation and systems are outdated, fragmented and do not fully align with constitutional principles of equality, non-discrimination and human dignity.

The integrity of the population register depends on the integrity of all the primary data systems, which must meet high standards of security, as specified in relevant Acts, and produce data that is accurate and reliable. While it is important to secure and modernise the DHA identity management system, the continued reliance on primary systems that are manual and insecure poses a serious risk to the accuracy of the population register. The following systems or processes provide primary data that is used to affirm identity or status to the applicant:

- Notification of birth from the Department of Health
- Notification of death from the Department of Health
- Notification of death from funeral undertakers
- Affidavits from traditional leaders and school principals for late registration of birth and claim for citizenship
- Abridged marriage certificates from religious marriage officers
- Divorce decrees from the Department of Justice and Constitutional Development
- Letter of non-impediment from a foreign country confirming that a non-citizen who intends to marry in South Africa is not married in the country of origin
- Police clearance form from a foreign country confirming that a non-citizen who is applying for a residence status in South Africa does not have a criminal record in the country of origin
- Bank statements from a foreign country confirming availability of the required bank balance in the account of a non-citizen who is applying for residence status in SA.

Figure 1 below illustrates some of these primary systems or processes that provide the critical information required by the DHA to affirm identity or status. These systems will continue to compromise the new population register if they are not modernised or secured.

Figure 2.1: An overview of the civic registration and vital statistics interface

Source: Statistics South Africa: South Africa's progress in civil registration

The DHA realises that the identification data at its disposal, including both civic status and immigration data, has a broader value than the core administrative purpose it currently fulfils. For instance, the DHA requires a regulatory framework for enabling e-government and e-commerce.

The DHA is currently operating without an approved identity management framework. This framework needs to address how the DHA will regulate the manner in which personal information will be processed by establishing conditions that meet the minimum threshold requirements for the lawful processing of personal information contained in the Protection of Personal Information (POPI) Act 4 of 2013. It will also be necessary for the DHA to articulate how the digital administrative datasets under its control will meet the requirements of both the contemplated privacy impact assessments in terms of POPI, and the cybersecurity audits in terms of the Cybercrimes and Cybersecurity Bill. Where the data handled by an organ of state qualifies as personal information that organ of state must establish a specific identity management policy to ensure compliance with POPI. Where an organ of state's system is classified as critical information infrastructure, a framework must be set in place to ensure compliance with the provisions of the Cybercrime and Cybersecurity Bill and independent audits of this must be undertaken from time to time.

The DHA, through both internal processes and external assessments, has confirmed and expressed the contextual, systems-related and operational problems and challenges in-house, within government and externally. The White Paper (December 2019) alludes to

the many factors constituting obstacles. It observes that, by 2016, it was evident that the DHA's existing operational, organisational and funding models were constraining the modernisation process with negative consequences for its sustainability and effectiveness. The White Paper further observes that the following three significant shifts had to happen to complete the modernisation process and deliver on the DHA's mandate:

i. Firstly, how the DHA is perceived must shift towards an understanding that its full mandate is a key enabler of citizen empowerment, economic development, efficient administration and broadly defined national security.
ii. Secondly, the DHA must be positioned as being central to building a capable State that can confront extreme inequality, poverty and the impact of 4IR.
iii. Thirdly, the DHA must realise its vision of becoming a fully modernised, secure department with professional staff (in the broad sense of the term) and appropriate operating, organisational and funding models.

The DHA as an institution in the current social, political, economic and global environment has to change and adapt. The reasons behind this change are:

- historical
- related to alleviating threats to the nation and are bound, significantly so, to the unfolding future that is fundamentally shaped by the adoption of advanced technologies
- evolved identity management that now has digital technology at its core.

In this context, the **historical legacy of the apartheid systems** that separated South Africans into different geographic and separate identity enclaves in the white Republic, ethnic homelands and self-governing territories is a factor to be considered. The apartheid ideology meant that the areas where the black majority population lived were severely underdeveloped and under serviced. Some of the daunting challenges the DHA faces are rooted in South Africa's history of a system that differentiated South Africans based on race and geographic origin and enshrined them in the separation of the former Republic of South Africa from the homelands and self-governing territories. This system was pursued through laws, regulations and practices that deeply politicised and racialised the allocation of resources and infrastructure, and building systems that could adapt to a changing global context. This bequeathed the post-apartheid government and the DHA with monumental challenges in infrastructure, systems and personnel.

In the DHA circumstance, the **technological advances shaping identity management and systems** are best represented by the change over decades from South Africa's Identity books of the early 1960s, where a fading photo, typed biographical information, handwritten entries and manual ink fingerprints imprinted on paper were the totality of what constituted identity. At the moment digital platforms and networks form the

backbone of the global financial enterprise that is led by financial institutions such as banks. Central to this is biometric data, which now includes fingerprints, iris reading, facial recognition and DNA, e-identity, e-government and e-commerce. The impact of these technological advances lies in how government services are provided and how governments facilitate and enable this widening economic activity.

National security and the protection of South Africa's sovereignty, the security of the State and citizens, and the integrity of the NIS is another factor. This comes from a number of considerations including the fight against the global threats of local and international crime syndicates and global terrorism, and taking steps to ensure that government services, on which multiple trillions of rand are spent, are enjoyed by those with rights and entitlements to them.

National developments in South Africa on identity management are linked to international developments, as changes and trends at the global level directly affect and influence South Africa's position and actions on identity management. South Africa's capability to facilitate and secure the application tourist and business visas, matched with migration control through a seamless digital system that employs modern and secure technologies and systems on identity authentication, stands to boost South Africa's economy through trade and investment in the country.

In South Africa providing and accessing goods and services that citizens and residents are entitled to depend on identity instruments issued by the DHA. This leads to a substantive policy, programme, implementation and operations relationship between the DHA and other government departments and State entities, based on the goods and services from the State to citizens. There are many stakeholders and actors in the area of identity management within and outside government. In the private sector, stakeholders, especially financial institutions, operate with business systems that require real-time verification services that are provided by the DHA through its legal mandate. Because of its multiple stakeholders and actors, and in promoting e-government through platforms for data sharing and processes, the DHA categorises several service-oriented streams of its work into:

- government to government programmes (G2G) – is concerned with interaction between different levels of government and collaboration with government agencies
- government to citizen programmes (G2C) – involves an interaction between government and its citizens
- government to employee programmes (G2E) – this involves the relationship between government and its employees. This form is considered an effective way of bringing employees together and promoting knowledge sharing among them

- government to business programmes (G2B) – this is concerned with supporting business activities.

Identity management has to be considered beyond South Africa's Borders. South Africa's own national developments on identity management have to take full cognisance of the fact that South Africa is part of the Southern African Development Community and the African continent through membership of the African Union. South Africa participates in the Southern African Development Community in areas such as identity management and financial transactions, the vision and policies of the African Union and Agenda 2063, and in multiple forums that are part of the international and global community. This means that ideas, views and developments from these forums will shape in remarkable ways the national South African agenda and practices in identity management.

2.2 Root cause analysis

The objective of this section is to assess the extent to which the challenges facing a secure and inclusive population register originate from a lack or insufficiency of a policy and legislative framework, and outdated and fragmented systems or administrative weaknesses.

2.2.1 Accessibility and barriers to inclusion

There are vulnerable groups that face significant economic and social barriers to enrolling in or using the South African identity system. Unless the identity system and its implementation are designed to help people overcome these barriers, it is likely these vulnerable segments of the population will have lower rates of coverage. While South Africa has made great strides towards ensuring that no one who lives in the country is left without a legal record of existence, there are still people (including citizens) who remain either undocumented or improperly documented. This group includes non-binary persons, people who did not acquire birth certificates earlier in life and now require late registration of birth, children of non-citizens who were born in South Africa, and those who are either excluded or improperly documented for historical reasons such as the borderline communities and KhoiSan people.

Abandoned children are excluded because of the requirement for identity details for parents at registration. Children abandoned by their parents are left in the care of their relatives who often do not have the required birth registration information. This means that the absence of a parent or legal guardian poses challenges for birth registration. There is a solution to this problem, but illiteracy and affordability issues worsen the situation. Children of teenagers who have not reached 16 years and do not have parents nor informants are unable to register the birth of their children. Children of asylum seekers who are not included in the file of the asylum seeker are excluded from the identity system

because of difficulty in providing documentation or other evidence such as paternity test for identity proofing.

Gender and sexual identity minorities are excluded because the current laws and policies do not cater for changes in the gender/sex attribute of the identity system. They experience discrimination when attempting to register or update their gender in the ID system.

Poor people, rural residents and many elderly people face logistical and travel challenges. The direct and indirect costs such as fees, travel and lost wages associated with the application for, or use of, identity credentials are prohibitive to them. They also lack smartphones or other resources to access online or digital services or use credentials. The elderly also have difficulty providing biometrics and have limited access, or literacy to access, digital services. Persons with disabilities also lack mobility and/or accessible centres, which may hinder registration. The DHA may also lack trained staff and accommodating enrolment procedures. People with lower levels of literacy have difficultly completing applications as forms are either written in English or Afrikaans. These barriers constitute a root cause for exclusion of vulnerable groups.

It is currently possible for anyone who has not applied for an ID (smart ID card or ID book) to successfully claim and use the identity of another person who has also not applied for an ID. This is possible because children's biometrics were not captured. The DHA currently has no way to reliably verify that a child who presents a birth certificate as proof of identity during interactions with the department, e.g. when applying for an ID for the first time, is truly the person whose birth the certificate is meant to certify. Any child can lay claim to the identity of another child and such instances have been recorded. For instance, there is a practice, especially in borderline communities, where birth certificates of deceased children are sold to foreign nationals. This happens when the death of a child is not reported to the DHA. The DHA aims to deal with this fraud by capturing children's biometrics when their births are registered to reliably verify their identities during subsequent interactions with the department and other institutions. However, not all biometric traits captured from children shortly after birth can be used to verify their identities later in life.

2.2.2 Interoperability and integration of identity management systems

Interoperability is crucial for developing efficient, sustainable, and useful identity ecosystems. Specifically, interoperability is the ability of different functional units – e.g., systems, databases, devices, or applications – to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units. The South African identity system itself does not have standards-based

technical interoperability and therefore does not allow different components and devices to communicate with each other and work together.

The DHA, in realising its mandate, uses the following core information technology (IT) systems to record, store and/or process citizens and non-citizens' biographic and biometric data, as well as their movements into and out of South Africa:

(a) NPR, which is used to record, store, and process citizens and permanent residents' biographic data, and limited biographic data for refugees
(b) National Immigration Information System (NIIS), which is used to record, store and process biographic, biometric and supporting data (audio files and scanned documents) of refugees and asylum seekers
(c) Movement Control System (MCS) and the Enhanced Movement Control System (EMCS), which are used to record and store the movement data of people across South African ports of entry. MCS is further used to record other data related to the movement of people across ports of entry, including visas, v-lists, etc.
(d) Visa Adjudication System (VAS), which is used to record, store, and process mostly biographic data and the supporting documents of people who apply for South African temporary and permanent residence permits in South Africa
(e) Visa system, which is used to record, store, and process mostly biographic data of people who apply for South African temporary residence permits at South African missions abroad
(f) Home Affairs National Identity System (Hanis), which is used to store and process the biometric data of citizens and non-citizens (refugees, asylum seekers, illegal foreign nationals and permanent residents). This system will be replaced in the immediate future by the Automated Biometric Identification System (Abis), which will process and store biometric data of all persons, citizens and non-citizens.

Therefore, the data of a person is, in most cases, stored on more than one system, e.g. the data of a citizen who has travelled outside South Africa exists on the NPR, and on the MCS and/or EMCS. In addition, the systems may store the same data in different ways, e.g. names.

However, the systems are generally not linked and do not communicate directly to exchange data; e.g., an update of the common data is not automatically updated on all the relevant systems that have the same data. This means that it is possible to change a person's ID number on the NPR without also changing the ID number on MCS (and/or EMCS). This effectively breaks the link between a person's data on the NPR and their data on the MCS (and/or EMCS), giving the appearance that the person has never travelled and rendering the person's data inaccurate.

The department plans to address this challenge and other data challenges by developing the NIS, which will be the single source of all DHA client data. It will consolidate the data stored on the NPR, NIIS, MCS, EMCS, VAS and the visa system into one database, and serve as the link between other systems and Abis, i.e. insertion of and access to the biometric data stored on Abis will be through the NIS.

2.2.3 Data protection and privacy

According to best international practice, ensuring data privacy and security requires a holistic approach to system design that incorporates a combination of legal, administrative and technical safeguards. South Africa has adopted general data protection and privacy laws that apply not only to the identity system, but to other government or private sector activities that involve processing personal data. Section 14 of the Constitution protects the right to privacy. The POPI Act regulates processing personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests. In a nutshell, the POPI Act aims to promote protection of personal information; give effect to the constitutional right to privacy; and prohibit unlawful collection, dissemination and use of personal information. It further provides a framework for handling personal information.

The Identification Act and Alteration of Sex Description and Sex Status Act 49 of 2003, are key legislation that regulate how personal data that is hosted in the DHA identity management systems is handled. The legislation needs to be amended to regulate handling personal information in line with the Constitution and the POPI Act. The current practice of dumping the department's data on other government systems is contrary to the POPI requirements.

2.2.4 Institutional oversight on data protection and privacy

International best practice dictates that data protection and privacy are subjected to the oversight of an independent supervisory or regulatory authority to ensure compliance with privacy and data protection law, including protecting individuals' rights. The POPI Act established the Information Regulator, an independent body subject only to the Constitution and to the law. This body is appointed by the President on the recommendation of the National Assembly, after nomination by a committee composed of members of all the political parties represented in the National Assembly.

The powers, duties and functions of the South African Information Regulator are aligned with the international best practice powers and duties. However, the Information

Regulator is not yet fully functional and able to legally deal with some key aspects of data protection such as data leaks. This is an institutional root cause for the lack of data protection and privacy.

2.2.5 Data security

In keeping with international best practice, personal information should be stored and processed securely and protected against unauthorised or unlawful processing, loss, theft, destruction or damage. This principle becomes increasingly important for digital identity systems given the threat of cyber-attacks. In South Africa, the POPI Act requires the Information Regulator, to notify the data subjects of breaches as soon as reasonably possible after the discovery that they have been compromised, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

2.2.6 Data sharing

According to international best practice, there are potential benefits of information sharing such as better government service delivery, improved risk management and cost savings as duplication of effort is eliminated. However, information sharing between state institutions, if not well regulated, can enable circumvention of individual privacy and data protection safety measures. The POPI Act effectively grants the right to privacy as contained in the Bill of Rights and is widely regarded as being a codification of the common law position regarding processing personal data.

2.2.7 User consent and control

In accordance with international best practice, an individual's personal data should only be collected and used with the consent of that individual unless there is another basis in law for such collection and use. There must be a valid lawful basis for processing personal data. One such lawful basis is consent of the individual. Where consent is relied on, it must be freely given, specific, informed, unambiguous and signifying agreement to personal data being processed. Where the personal data being processed is special category data such as biometric data, additional conditions to processing must be satisfied, one of which is obtaining the individual's explicit consent to the processing.

Explicit consent must be provided in a clear statement – whether written or spoken. An explicit consent statement will also need to specifically refer to the element of the

processing that requires explicit consent. The POPI Act makes the provision that personal information may only be processed if the data subject or a competent person – where the data subject is a child – consents to the processing. The POPI Act also states that the responsible party bears the burden of proof for the data subject's or competent person's consent.

2.2.8 Cybercrime and cybersecurity

Cybercrime may have a wide range of meanings depending on the country, legal instrument and context in which the phrase is used, but according to best international practice, a country should have laws in place addressing criminal conduct directed against the confidentiality, integrity and availability of computer systems and networks, as well as the data stored and processed on them, and criminal acts carried out through the instrumentality of such systems, networks and data. South Africa currently does not have any legislation on cybercrime and cybersecurity. Since 2015, the government has been working on cybercrime and cybersecurity legislation with the stated aim of bringing South African law in line with international standards and creating specific offences for cyber-related crime such as online fraud, forgery, extortion and terrorism.

In 2017, Parliament began deliberations on the Cybercrimes and Cybersecurity Bill. The 2017 version of the Bill contained a provision concentrating cybersecurity powers in the hands of intelligence agencies and potentially criminalising free expression. In October 2018, Parliament began deliberations on a significantly revised version of the Bill, referred to as the Cybercrimes Bill. However, the Bill has yet to be adopted by both houses of Parliament and signed into law, which is a root cause for the lack of cybercrime and cybersecurity legislation.

2.2.9 Identity authority and governance structure

Identity authorities are specialised entities responsible for implementing and/or overseeing personal identity data collection, verification, storage and sharing; issuing credentials, and verifying and authenticating identity data. They are also typically responsible for public engagement and redressing grievances. For an identity system to succeed, this entity must be empowered by law and political will and should demonstrate the capacity to serve as a champion of identity, a convener of multiple stakeholders and an effective implementer and/or overseer.

In South Africa, civil registration and the NIS operate under the auspices of the same entity – the DHA – which is responsible for civil registration and national identification, immigration and border management, and refugee management. The DHA is therefore a

single, dedicated entity for identity management in South Africa, yet South Africa does not have a legislation that identifies and affirms the DHA as the sole provider of official identity management services. There are other entities within and outside government that are providing related services.

However, the DHA appears not to be well equipped with sufficient and capable human, financial and technological resources to efficiently carry out its mandate, implying a potential institutional root cause for not administering official identity management.

Chapter 3: Policy development approach

3.1 Scope

The policy will provide a constitutionally sound framework for regulating the following critical elements of identity management:

- Recognise equality, non-discrimination and human dignity values in managing the official identity and status of all citizens and non-citizens who interface with the DHA.
- Recognise the identity number, identification credentials (birth certificate, identity card/document and passport) and biometric data as the sole sources for verifying citizen identities.
- Recognise the passport number, identification credentials (visa and permit) and biometric data as the sole sources for verifying identities of foreign nationals within South Africa's territorial jurisdiction.
- Recognise the identity number and biometric data as the sole sources for accessing government services such as social services and for paying tax.
- Reposition the DHA as the sole provider of official identity and civic status verification services.
- Establish rules that govern accessing and processing population register data in line with relevant policies and legislation.
- Replace the NPR with an inclusive, digital population register that is secure, accurate and confidential.
- Establish the NIS to interface with other government identity management systems and generate the critical data needed by e-government and e-commerce to function.
- Apply for DHA services via multiple digital channels.

3.2 Out of scope

The Official Identity Management Policy does not deal with the following policies or processes:

- Policies and processes to attain citizenship

- Policies and processes to attain immigration status in the country
- Policies and processes to grant refugee status
- Policies and processes to determine who qualifies for which government services.

It is important to emphasise the following principles as we develop the policy:

- No one, irrespective of their status, should be left without a legal record of existence **(scandal of invisibility)**
- Being included in the population register does not translate to any status (immigration or citizenship) other than that your identity is properly documented in the country.

3.3 Policy objectives

This policy is developed with the following objectives in mind:

- Enable an inclusive digital population register that is secure, accurate and confidential
- Position the DHA as the sole provider of official documentation relating to the identity of civic and international migration status of citizens and foreign nationals within South Africa's territorial jurisdiction
- Position the DHA as the sole provider of official identity and civic status verification services
- Establish rules that govern accessing and processing population register records and data in line with relevant policies and legislation such as the POPI Act and the Cybercrimes Bill
- Establish the NIS to generate critical data needed for e-government and e-commerce to function
- Enable an application for DHA services via multiple channels.

3.4 Methodology

Globally there are a number of organisations and forums that investigate identity management and identity management systems. The World Bank, with its Identification

for Development initiative working with many global partners, has become an indispensable resource on identity management.

As part of the process of developing a policy on identity management, the DHA researched and analysed international and regional developments in identity management. The research surveyed the systems and practices of countries that are considered internationally to be advanced, intermediate or emerging in their development of secure, digital and interoperable NISs. The research collected information at international and regional levels and also explored the key documents and studies carried out in different regions and countries of the world. The approach was to look at the following seven dimensions in each of the countries investigated.

i. Description of the national identity management system
ii. Establishment of the national identity management system
iii. Management of the national identity management system
iv. Digitalisation of the identity management system
v. Maturity of the national identity management system and integration with other services
vi. Data sharing and processes or procedures governing access to national identity
vii. Statistics on coverage of the identity management system.

The international and regional analysis demonstrated the complex, evolving social, economic and technology-driven environment with multiple stakeholders and actors in identity management systems.

The seven dimensions were then applied to the South African context.

The research was complemented by a comprehensive consideration of national developments in South Africa on identity management and related challenges. The outcome pointed to the current status at DHA and the multiple challenges that have to be addressed on the path to a modern and secure NIS and an identity management policy. National developments highlighted the need for integration and building synergies within government, and for enhancing and strengthening the interface with private sector institutions by exploiting modern secure technology. This process culminated in the first draft of the Identity Management Policy being developed.

SECTION B: OVERVIEW OF IDENTITY MANAGEMENT IN SA

Chapter 4: Evolution of identity management

4.1 Introduction

This section considers the interplay between national, regional and international developments on identity management. Under these circumstances, the DHA has to respond to broader national and international issues and global developments on identity management. This translates into the DHA adapting, adopting, using and exploiting that which serves South Africa's national interests.

In the post-apartheid period since 1994, the DHA has undergone several phases in terms of its strategic goals, focus of functions and operations. The historical legacy of the apartheid systems with the then Republic of South Africa, the TBVC states and self-governing territories meant that the attention was on building a unitary State with one single central authority. Consequently, the years 1994 – 2007 saw the DHA driven by the imperative to bring all South Africans into a single NIS by registering all citizens of the new Republic South Africa into one NPR. This critical initiative was accompanied by extending and expanding DHA services to areas that were historically underserved in terms of both infrastructure and services. Today, the DHA has mobile units that reach areas without infrastructure and is a remarkable and innovative method for taking services to all South Africans and advancing the agenda and principle of inclusivity.

4.2 Modernisation programme

The current DHA systems are not integrated and many processes are largely paper-based. Changes to identity and status that are made in immigration systems are only partially reflected in the NPR, using lengthy manual processes that are not reliable. The NPR was designed in the 1980s and data is often inconsistent or missing. Biometric and biographical data are stored on a mixture of paper and digital records that are neither reliable nor sufficiently secure. The existing operating model is based on one used before 1994 by "white" Home Affairs, characterised by clients queuing before a front office clerk to complete forms.

The DHA initiated a modernisation programme in 2012 with the aim of integrating and digitising its systems, and transforming its delivery systems to achieve the strategic objectives of inclusivity, national security, service delivery and meaningfully contributing to the government-wide agenda of a growing, inclusive economy. The goal

of the modernisation programme is to build a Home Affairs that has replaced its legacy systems with multiple channels and integrated digital systems. The assumption is that these systems will be very secure, professionally managed and appropriately funded.

The new DHA systems and operating model will be built around the new NIS and linked to the systems for the civil registration of birth, nationality, citizenship, marriage and death. It will also be linked to the MCS and other immigration systems. The NIS will enable the DHA to manage all its functions efficiently and responsively, as the NIS will link the identity of all citizens and other persons in a country to their civil and immigration statuses. Interfaces between systems will mean that data is accurate and continually updated in real time.

The modernisation programme consists of multiple projects: short-, medium- and long-term. Elements that are being rolled out include the smart ID card, fully digital ID and passport processes, online capture of biometrics at ports of entry and upgrades to the movement control and biometric systems. An automated system for asylum seekers to make appointments was designed and installed by the DHA at the newly opened Desmond Tutu Refugee Centre, greatly reducing fraud and human rights abuses and increasing efficiency. An in-house contact centre was opened in 2015/16, which was one of the key elements of the new operational model.

Given its limited resources, the DHA has entered into partnerships to improve access by creating new channels. A partnership agreement with the major banks allows their clients to access a DHA service point. They apply and pay for a smart ID card or passport online and make an appointment to complete the process at a bank. An SMS advises them when to collect the document at the bank. A partnership with a visa facilitation service led to the company creating service points in several countries abroad and in major South African cities. Applications are sent digitally to the DHA, where adjudicators complete the process. Together with local development agencies, the DHA has extended the service to create one-stop centres for businesspeople in major cities.

This third phase of the DHA's transformation promises a clear path towards digitisation and attaining a paperless environment. In a nutshell, the achievements of the modernisation programme include the following:

- Automated ID and passport processes into Live Capture
- Rolled out the Live Capture system to 193 offices
- Integrated and updated the payment system into the Live Capture system
- Enabled online services through the new eHomeAffairs portal
- Rolled out capturing smart ID cards and passports with the banks
- Rolled out smart ID cards, with the milestone of more than 12 million cards reached in March 2019
- Established a new contact centre

- Implemented online verification, resulting in birth, marriage and death certificates and temporary IDs being issued on the spot
- Deployed the Queue Management System at Live Capture offices
- Implemented the EMCS at 70 ports of entry
- Implemented a paperless process at Marabastad, now Desmond Tutu Refugee Centre
- Abis to replace Hanis
- Launched the e-visa system.

4.3 Repositioning programme

Repositioning the DHA from administration to key contributor to strategic national security came about in March 2017, with Cabinet approval. Central to this new security-related mandate is the capability of the DHA to protect South Africa's people, systems and data. The DHA has identified the following overriding strategic objectives:

- Establish and maintain a secure, comprehensive and reliable register of the identity and status of all citizens, as well as all foreign nationals in South Africa.

- Establish and maintain a secure and efficient system of immigration management that is used strategically to minimise risks and maximise the benefit of immigration.

- Establish and maintain world-class standards in delivering secure and reliable identity, civil registration and immigration services by patriotic, professional and caring staff.

- Establish a Home Affairs that has the policies, people, processes and infrastructure required to secure its systems and deliver world-class services.

Chapter 5: Current policy and legal framework

A number of policies and legislation have an impact on official identity management.

5.1 Policy framework

- **Constitution of South Africa 1996:** The Constitution of South Africa provides for the right to privacy in terms of the common law and section 14.
- ***White Paper on Home Affairs* 2019:** Through this proposed White Paper, the DHA is positioning itself to deliver effectively against its mandate as a critical enabler of citizen empowerment, economic development, national security and an efficient State.
- ***White Paper on Science, Technology and Innovation* 2018:** This White Paper focuses on using Science, Technology and Innovation to assist in solving problems that, among others, are associated with rapid technological advancement, geopolitical and demographic shifts, and 4IR.

5.2 Legal and regulatory framework

5.2.1 DHA internal:

- **Alteration of Sex Description and Sex Status Act 49 of 2003:** This Act provides for altering the sex description of certain individuals under certain circumstances, amends the Birth and Deaths Registration Act 51 of 1992 as a consequence, and provides for matters incidental to this.
- **Births and Deaths Registration Act 51 of 1992:** This Act provides for the compulsory registration of births and deaths for both South Africans and non-South Africans.
- **Citizenship Act 88 of 1995:** This Act provides for the acquisition, loss and resumption of South African citizenship.
- **Identification Act 68 of 1997:** This Act regulates compiling and maintaining a population register of the population of the Republic, for issuing identity cards and certain certificates to persons whose details are included in the population register.
- **Immigration Act 13 of 2002:** This Act provides for regulating the admission of persons to, their residence in, and their departure from, the Republic.

- **South African Passports and Travel Documents Act 4 of 1994:** This Act provides for issuing passports and other related travel documents to South African citizens.

- **Refugee Act 130 of 1998:** This Act gives effect within the Republic of South Africa to the relevant international legal instruments, principles and standards relating to refugees. It also provides for the reception of asylum seekers into South Africa, regulates applications for, and recognition of, refugee status and provides for the rights and obligations flowing from such status.

5.2.2 DHA external:

- **Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000:** This Act provides for the prohibition of unfair discrimination based on race, gender, sex, pregnancy, family responsibility or status, marital status, ethnic or social origin, HIV and AIDS status, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth.

- **Cybercrimes Bill 2019**: This Bill will create offences that have a bearing on cybercrime, will criminalise the distribution of data messages that are harmful and provide for interim protection orders. The Bill will regulate jurisdiction for cybercrimes, regulate the powers to investigate cybercrimes and impose obligations to report cybercrimes. In addition, the Bill will provide for capacity building, will provide that the executive may enter into agreements with foreign States to promote measures aimed at detecting, preventing, mitigating and investigating cybercrimes, and will provide for deleting and amending the provisions of certain laws.

- **Electronic Communications and Transactions Act 25 of 2002:** This Act provides for facilitating and regulating electronic communications and transactions. It provides for the development of a national e-strategy for the Republic. It also promotes universal access to electronic communications and transactions and the use of electronic transactions by small, medium and micro-sized enterprises. In addition, the Act prevents abuse of information systems and encourages the use of e-government services.

- **Promotion of Access to Information Act 2 of 2000:** This Act gives effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for to exercise or protect any rights. The Act also gives effect to the constitutional right of access to any information held by the State, and any information that is held by another person and that is required to exercise or protect any rights.

- **Promotion of Administrative Justice Act 3 of 2000:** This Act focuses on ensuring that administrative bodies act reasonably and procedurally fairly. It stipulates that any decisions by an administrative body can be challenged in court if such an action is, among other things, procedurally unfair, not within an entity's powers set out in law, biased "or reasonably suspected of bias". It also allows for administrative bodies to be taken to court for "failure to take a decision".

- **Protection of Personal Information Act 4 of 2013:** This Act promotes the protection of personal information processed by public and private bodies. The Act gives effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information. This Act also provides persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act The Act establishes voluntary and compulsory measures, including establishing an Information Regulator, to ensure respect for, and to promote, enforce and fulfil, the rights protected by this Act.

- **Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002:** This Act regulates the interception of certain communications, monitoring certain signals and radio frequency spectrums and providing certain communication-related information. The Act regulates making applications for, and issuing, directions authorising the interception of communications and the provision of communication-related information under certain circumstances. It also provides for prohibition of manufacturing, assembling, possessing, selling, purchasing or advertising certain equipment, and creates offences and prescribes penalties for such offences.

- **State Information Technology Agency Act 88 of 1998:** This Act provides for establishing a company that will provide information technology, information systems and related services to, or on behalf of, participating departments and regarding these services, act as an agent of the South African government.

- **The Public Services Act 1994:** This Act empowers the minister of public services and administration to develop and establish norms and standards related to, among others, information management and electronic government in the public service.

SECTION C: POLICY FRAMEWORK AND OPTIONS

Chapter 6: Policy framework

Vision

The Official Identity Management Policy is one of the founding policies that give effect to the vision of the DHA: a South Africa where identity, status and citizenship are key enablers of citizen empowerment and inclusivity, economic development and national security.

Principles

The shared principles[3] outlined below are influenced and derived from the World Bank principles on identification for sustainable development. They are also informed by the Constitution and other transversal legislation such as the POPI Act. These principles set out considerations for developing a regulatory framework that maximises the benefits of an identity management system while minimising its risks. They are intended to maximise the benefits of an identity management system.

In this regard, it is recommended that a policy and legislative framework should, at a minimum, incorporate **10** principles under the following **three** themes:

- Inclusion (universal coverage and accessibility)
- System design (robust, secure, responsive and sustainable)
- Governance (building trust by protecting privacy and user rights)

These three themes are discussed and expanded into the principles as follows:

6.1 Inclusion

The identity management system should recognise all persons and should not discriminate on any specific grounds, such as gender, race, religion, political affiliation,

[3] Principles on Identification for Sustainable Development: Towards the Digital Age (2017), facilitated by the World Bank and Centre for Global Development

etc. Inclusion means treating citizens and non-citizens fairly. For the identity management system to be inclusive, it must ensure integration of all users.

Inclusion entails the following principles:

- Ensuring universal coverage for individuals from birth to death, free from unfair discrimination
- Removing barriers to access, usage and disparities in the availability of information and technology.

6.2 System design

Identity management systems should be robust, context appropriate, and interoperable. While they should respond to user demand and long-term needs, they should collect and use only the information necessary for the system's explicit purpose. Open standards and vendor neutrality help to ensure financial and operational efficiency and sustainability.

The data or information and privacy of individuals must be protected in the country's Constitution. The identity management system should be designed with the privacy of the end-user in mind. No action should be required on the part of the individual to protect his or her personal data. Information should be protected from improper use by default. The right to privacy should be protected by law. The law should ensure that the collection and use of personal data or information is protected. The design of the regulations should ensure that the data subject is informed of the purpose and intended use of the data that is collected. To ensure prevention of leaks and loss or theft of data or information, the regulations should require physical, technical and administrative protection of data or information.

Design entails the following principles:

- Establishing a robust, unique, secure, and accurate identity
- Creating a platform that is interoperable and responsive to the needs of various users
- Using open standards and ensuring vendor and technology neutrality
- Protecting user privacy and control through system design
- Planning for financial and operational sustainability without compromising accessibility

6.3 Governance

Consent is the basis for good governance of the identity management system. There should be regulations that specify consent as the basis for collecting and using personal data or information. Therefore, it is a recognised general rule that personal data or information should only be used on receipt of consent from the owner. The regulations should provide for the right to access, rectify and/or delete personal data about the owner held by third parties. Furthermore, there should be at least one administrative authority that has a responsibility to protect personal data/privacy.

Governance entails the following principles:

- Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework
- Establishing clear institutional mandates and accountability
- Enforcing legal and trust frameworks though independent oversight and adjudication of grievances.

The above principles will guide the department in developing the new identity management policy and legal framework.

Chapter 7: Policy analysis and options

This chapter is the backbone of the Official Identity Management Policy. It introduces policy options that will be translated to a policy proposal when the policy paper has been approved by Cabinet. Policy options are discussed under each principle.

7.1 Principle 1: Ensuring universal coverage for individuals from birth to death, free from unfair discrimination

The universal coverage principle requires countries to **fulfil their obligations to provide legal identification to all residents—not just citizens—from birth to death**, as set out in international law and conventions and their own legislative frameworks. This includes the commitment to universal birth registration for those born in their territory or jurisdiction. It also includes **linking civil registration and identity systems**, which is an essential part of ensuring the accuracy and sustainability of identity systems. In addition, identity systems should be **free from unfair discrimination**.

This requires practitioners to identify and mitigate legal, procedural and social barriers to enrol in and use identity systems, with special attention to poor people and groups who may be at risk of exclusion for cultural, political or other reasons (such as women and gender minorities, children, rural populations, ethnic minorities, linguistic and religious groups, persons with disabilities, migrants, the forcibly displaced and stateless persons). Furthermore, identity systems and identity data should not be used as a tool for discrimination or infringe on individual or collective rights. While **secure and inclusive identity systems** are essential for ensuring that no one is left behind without a legal record of their existence, they are not a **guarantee for a change of status such as citizenship and immigration status.**

7.1.1 Lack of birth registration for all

Finding and cause: In South Africa, inclusion is high with near universal coverage of all persons in the Republic. A gap was identified in the **registration of all** births onto the NPR. This is caused by the **absence of a clear policy and legislation that governs the registration of all different categories of persons** in the NPR and other immigration systems.

The Identification Act, which establishes the NPR, only caters for issuing birth certificates and ID cards to citizens and permanent residents. As a result, the personal information (identity and status) of other people such as international migrants is not stored on the NPR but on other immigration systems that are not linked to the NPR. The

current practice is that children born to non-citizens are issued with birth notification forms that are not included on the NPR and, thus, cannot be tracked and traced.

The Identification Act and Births and Deaths Registration Act do not cater for the birth registration of children who are born intersex. Such children are assigned either a male or female sex status at birth. Some social groups are discriminated against in the current identity management system. This is because the identity number that we use is not gender neutral. The identity number recognises and accommodates only two categories, namely, male and female. The ID system does not differentiate between the distinct concepts of sex and gender. The World Health Organization defines sex as "the different biological and physiological characteristics of males and females" and gender as "the socially constructed characteristics of women and men"[4]. Whereas gender is traditionally thought of as a binary attribute (male vs. female), a third gender is now being increasingly considered (intersex). If an individual transitions to a new gender, the ID system should be updated. In fact, the Identification Act refers to gender and not sex.

The following **observations and policy options** apply under the principle:

i. Every birth that takes place in the country, irrespective of the status of the parents, must be registered. If technology and medical conventions allow, the biometrics of children must be captured at birth. Where impossible, the biometrics of a parent must be linked to the birth certificate of a child.

ii. The NIS must enable the creation of sub-database systems for registering births of citizens and non-citizens.

iii. The new legislation and NIS must enable the registration of births for intersex children.

iv. The identity number of a child must be processed on the basis of biographic information and linked to their parents' identity numbers and mother's biometric data.

v. When possible, the biometrics of a child must be collected at birth. A facial photograph must be taken for manual identification when needed. Children must be reregistered when they reach age five with ten fingerprints and iris and facial photographs.

vi. A combination of different biometric data for children should be considered with options such as the photograph of the ear. This depends on availability of proven technology.

[4]See World Health Organization, Gender equity and human rights, Glossary.

vii. The new legislation and population register must make a provision that enables the establishment of a category that is neither male nor female. That is, a sex category that caters for biological males with feminine gender identity or expression or biological females with masculine gender identity or expression in the identity system.

viii. The sex category must cater for transgender that will enable updates of sex information in the population register.

ix. The other option is to issue a random unique identity number that is not linked to or founded on a person's sex, date of birth, place of birth or any other marker.

Unintended exclusion of birth registrations is also caused by the lack of coverage, resource capacity and constraints of the systems, and weak cooperation between the Department of Health and the DHA. The following **observations and policy options** apply under the principle:

i. There has to be a stronger cooperation between the DHA and the Department of Health on birth notification and birth registration, with a reasonable presence of the DHA services at the facilities of the Department of Health where births occur.

ii. Securing of the Department of Health information system is very crucial since it is the main feeder system to the birth registration records held on the NPR. This can make significant contributions to enhancing the security and authentication of births.

7.1.2 Lack of death registration for all

Finding and cause: There are still cases of **unintended exclusion of death registrations.** Some communities **fail to notify the appropriate authorities** when death occurs and burials are undertaken without an official death certificate issued. Law enforcement of the mandatory process in the instance of death and burial is absent in some instances. The consequence of not registering deaths is that a person's record remains on the NPR as if the person is still alive. Thus, the NPR has a record of people who are more than 140 years old who are still recorded as alive. The other consequence is that a birth certificate of a deceased person can be sold to another person; this is enabled by the fact that the birth certificate is not linked to the biometrics of either a parent or a child.

The following **observations and policy options** apply under the principle:

i. In terms of law, death must be registered within 72 hours. Burying a person without a death certificate will be illegal to protect the integrity of the population register, ensure an accurate death register and prevent fraudulent use of birth and ID documents of the deceased.

7.2 Principle 2: Removing barriers to access and use of IDs, and removing disparities in the availability of information and technology

To ensure universality, principle 2 advocates eliminating barriers to accessing and using an ID. This includes removing or reducing direct and indirect costs for identification. Civil registration and first birth and death certificates should be free of charge to the individual, as should the initial issue of any identity credential that is mandatory – de jure or de facto – to possess or to access basic rights and services. If fees are charged for certain additional services (such as reissuance of lost credentials), rates should be reasonable, proportional to costs incurred, and transparent to the public. Consideration should be given to subsidising or waiving fees for poor and vulnerable persons. The indirect costs of obtaining identification – including fees for supporting documents, travel costs, and cumbersome administrative procedures – should also be minimised. For example, ID-related services should be available online and should routinely visit remote communities.

Furthermore, practitioners should **mitigate information disparities and the digital divide** by working to ensure user literacy regarding ID systems, fostering a culture of understanding and trust, and reducing information asymmetries that might prevent individuals from accessing identification-related services or benefits. With the rise of digital systems, no one should be denied identification or associated services because they lack mobile or internet connectivity or digital literacy. Stakeholders should work together to ensure both online and offline infrastructure can be extended to provide "last-mile" access and connectivity, particularly for those in rural and remote areas.

7.2.1 Removing barriers to access and usage

Finding and cause: Individuals that **cannot afford** registration services face a barrier that excludes them from the identity management system. The **cost barriers** (cost of identity cards, documents, etc.) lead to exclusion of individuals from the ID management system.

The following **observations and policy options** apply under the principle:

i. Citizens carry a duty and responsibility to protect identity documents/cards and keep them safe.

ii. Fees should only be charged for non-mandatory identity credentials such as passports. Replacements for lost or damaged cards should be charged on a sliding scale based on the number of replacements, with exemptions being available to persons with disabilities, the poor, senior citizens, children below age, victims of

natural disasters and persons who lost their cards as a result of being a victim of crime.

iii. The DHA must develop an indigent policy as part of a costing model. This policy must also cater for those who already hold green ID books but cannot afford to pay for the new secure smart ID cards.

iv. No one, irrespective of their status, should be left behind without a legal record of existence.

v. Being included in the population register will not translate to any status other than that your identity is properly documented in the country.

7.3 Principle 3: Establish a robust, unique, secure, and accurate identity

Principle 3 highlights that **accurate**, up-to-date information is essential for a trustworthy identification database and credentials used for authentication. Foundational identity systems should provide a **unique identity** that is verifiable over the course of a person's life, from birth to death. That is, within a foundational identity system, each person should have only one identity, and no two people should have the same identity. In addition, identity systems must have safeguards against tampering (alteration or other unauthorised changes to data or credentials), identity theft, data theft and misuse, cybercrime and other threats occurring throughout the identity lifecycle).

Finding and cause: Under this principle a number of gaps were identified and several findings were made.

i. The continued use of paper-based green ID card books increases risk of identity theft.

ii. Issuing paper-based birth certificates that cannot be linked to a child increases the risk of fraud.

iii. The legal age at which a person can apply for an identity documentation is 16 years. This is a serious risk since a person's biometrics are only collected when they apply for an ID. This situation has been exploited by criminals who steal the birth certificates or use minors as accomplice in criminal activities.

iv. The current identity system contains duplicate ID numbers and ID numbers that change when a date of birth is corrected or sex alteration takes place.

v. Identity credentials in different formats transact on multiple platforms are lacking.

vi. The address details on the NPR are outdated.

This situation arises from the continued use of manual and paper-based processes, systems and documents. The current application process for ID books and birth certificates at outdated offices, and fraud and corruption, add to the challenges. Undocumented unregistered South African child deaths are abused. Inadequate proofing measures prevail that lead to duplicate registrations. The systems are not integrated in the absence of digital platforms for multiple formats of credentials and the Identification Act not being enforced.

The following **observations and policy options** apply under the principle:

i. The department must intensify its strategy implementation for phasing out green barcoded ID books.

ii. The department must intensify its strategy implementation for modernising all its offices (frontline and back-office) to enable automation of all application processes.

iii. Once identity data has been collected through the registration process, it must be proofed to determine its veracity. The identity proofing process is fundamental to ensuring accurate and trustworthy identities are created.

iv. The two fundamental processes for identity proofing registrations are:

- **Validation:** Checking the validity, authenticity and accuracy of supporting documents or evidence provided and confirming that the identity data is valid, current, and related to a real-life person.

- **Deduplication:** Using biometric recognition (using biometric identification to identify other identities already registered that could be a match) and/or demographic deduplication algorithms to ensure that a person is unique.

v. In any identity system, identifying numbers are the most basic type of identifiers. In the context of foundational systems, ID numbers are considered to be unique when:

- The number-generating process ensures that no two people within the system share the same number.

- A deduplication process ensures that the same person does not have multiple identity records or numbers (that they are unique in the database).

vi. The **structure of an ID number**, including its format and length, require careful consideration of country context and privacy concerns. Policy options guiding the number structures to be used could include the following:

- A random number generated using mathematical algorithms and containing no

information about the person.

- A serial number assigned based on the order of entry into the system, with the highest number assigned to the most recent enrollee.
- A coded number that contains information about the person, with certain digits coded based on attributes such as birth year, sex, nationality, and location of application. That is, retain the current ID number but have three sex categories – male, female and intersex.
- The format of the new ID number must be as inclusive as possible, especially when it comes to intersex and transgender persons.
- The seventh digit of the ID number is a gender marker that indicates whether the ID holder is a female or a male – (0-4 means the holder of the ID is a female while 5-9 means the holder of the ID is a male). This is the most contentious digit for non-binary or transgender persons as it does not reflect their sexual orientation or gender. To accommodate non-binary, transgender and intersex persons, it is recommended that an alternative digit or letter "**X**" be used for this population. This will be a subject of further consultation with the affected population. This change will not affect the current composition of the ID number for males and females.

vii. In the digital era, however, randomised numbers are the preferred choice for enhancing privacy and security. Connectivity between registration points, along with the centralised nature of deduplication and advanced computing power, mean that it is now possible to assign unique, random numbers to every person in the ID system. Random numbers offer three primary benefits over coded numbers:

- They reveal no personal information. By definition, coded numbers reveal information about a person.
- They are more secure. Coded numbers make it easier for fraudsters to guess an ID number by narrowing down the possible combinations based on a few known facts about a person.
- They are immutable. In some cases, coded numbers contain information, such as nationality, place of residence, or gender, which may be subject to change over an individual's lifetime, requiring the numbers to be updated.
- The legal age for smart ID card application must be lowered to enable biometrics to be captured earlier and to curb identity theft. It is recommended that 10 years should be a new legal age for ID applications – this can be lowered further, but this age will mitigate a risk of having matriculants who write matric examinations

without smart ID cards.

7.4 Principle 4: Creating a platform that is interoperable and responsive to the needs of various users

Principle 4 highlights the need for identification and authentication services to be **flexible, scalable, and meet the needs and concerns of people (end-users) and reliant parties** (e.g. public agencies and private companies). The value of identity systems is highly dependent on their interoperability with multiple entities, both within a country and across borders. Domestically, this includes the ability of different databases or registries (e.g. foundational and functional databases) to communicate with each other, exchange data, and facilitate identity queries in a timely and low-cost manner, subject to appropriate privacy and security safeguards. It also includes **interoperability across borders** to facilitate mutual recognition of physical or digital IDs issued by one country in other countries, which can increase trade and enable safe and orderly migration.

Finding and cause: The finding was that there are no linkages between database systems within the civic services and immigration branches and little interlinkages and integration with other databases and systems within the DHA. Developing different identity systems (silo or fragmented identity systems) by different government departments leads to process duplication, increased costs and inefficiencies within government. Citizens are registering in different identity systems at various government departments and institutions.

This is because the approach to digital transformation adopted by different branches and government departments is not synchronised. Most existing systems were not designed to share information across branches and government departments.

The following **observations and policy options** apply under the principle:

7.4.1 Interoperability

Interoperability is crucial for developing efficient, sustainable, and useful identity ecosystems. Specifically, interoperability is the ability of different functional units such as systems, databases, devices, or applications to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units. Interoperability occurs at three levels:

- **Between identity subsystems**. Within the identity system itself, standards-based technical interoperability allows different components and devices to communicate with each other and work together.
- **With other domestic systems**. Identity systems must be interoperable with other

systems such as the civil registry and service providers that are reliant parties of the system to exchange data or facilitate queries. Communication with other systems may be provided through various interoperability layers, web services and APIs, or direct connections.

- **With identity systems in other jurisdictions**. Cross-border frameworks for interoperability and mutual recognition allow credentials from one country to be accepted in other countries. This includes, for example, accepting standards-compliant passports across the globe and regional frameworks for mutually recognising identity credentials.

- Legal, policy and regulatory frameworks should define the scope of interoperability, particularly with regard to data exchange and requirements for privacy and data protection.

The following **observations and policy options** apply under the principle:

i. Adopt one official identity management system across all government departments to store biographic and biometric information for citizens and non-citizens.

ii. Integrate all identity management databases in the new identity management system, the NIS.

iii. Create an e-government platform that will allow electronic verification and authentication services.

iv. Maintain separate identity management systems and create linkages between different identity management systems.

South Africa should constitute a focal point for identification services to help coordinate the approaches and activities of the several government entities that constitute the system as well as support from funding institutions. The focal point could be complemented by a user group representing several of the system's major customers such as the Department of Health, the South African Police Service, the Department of Social Development, etc.

7.4.2 Integration across borders

South Africa's identity management systems are not integrated and interoperable with those of neighbouring countries, as is the case with the Economic Community of West Africa States countries and the European Union. This is because there is a lack of cross-border integration and interoperability frameworks. Cross-border frameworks allow for interoperability and mutual recognition of countries' identity management systems.

7.5 Principle 5: Using open standards and ensuring vendor and technology neutrality

Principle 5 emphasises the need for **vendor and technology neutrality** to increase flexibility and avoid a system design that is not fit for purpose or suitable to meet policy and development objectives. This requires robust procurement guidelines to facilitate competition and innovation and prevent possible technology and vendor "lock-in," which can increase costs and reduce flexibility to accommodate changes over time. In addition, open design principles enable market-based competition and innovation. They are essential for greater efficiency and improved functionality in identification systems, and for interoperability.

Finding and cause: Identity databases are duplicated and there are large-scale system incompatibilities within government departments. A number of government departments are using diverse applications, platforms, software and databases that are vendor or product locked. Most of the existing ICT systems were not designed to share information across departments. This arose because common standards were not adopted within the DHA and among government departments.

The following **observations and policy options** apply under the principle:

i. Adopt open standards to ensure vendor and technology neutrality.

ii. ISO 29794-part 5: The new expanded standard on facial biometrics.

iii. ISO/IEC JTC/1 SC/17 SG/2: A special group on standards for virtual identity.

iv. Digital travel credential: Looks at both policy and technology and is coordinated between the International Civil Aviation Organization (ICAO) and ISO.

v. Standards-based ("plug and play") procurement model.

vi. XML advanced electronic signatures standard (XAdes).

vii. ICAO identity applet.

7.6 Principle 6: Protecting user privacy and control through system design

Principle 6 emphasises that identity systems must protect people's privacy and control over their data through system design. Designing with people's privacy in mind means that **no action should be required on the part of the individual to protect his or her personal data**. Information should be protected from improper and unauthorised use by default, through both technical standards and preventative business practices. These

measures should be complemented by a strong legal framework (as emphasised in principle 8).

For example, data collected and used for identification and authentication should **be fit for purpose, proportional to the use case**, and managed in accordance with norms for data protection. Credentials and numbering systems **should not unnecessarily disclose sensitive personal information**.

Finding and cause: Presently, user privacy is not protected in compliance with some sections of the POPI Act and there are no control mechanisms to ensure that users have access to the data contained in the ID system. This is a management issue as full compliance with the POPI Act is mandatory. The non-protection of user privacy is linked to the fact that some provisions of the POPI Act are not yet effective.

The following **observations and policy options** apply under the principle:

i. Privacy-enhancing technologies and security measures should be built into every aspect of the NIS by adopting a privacy by design approach that adheres to the foundational principles of privacy by design.

ii. Maintain user privacy and secure systems that process, collect, store, use, and disseminate personal data as this is a fundamental concern for ID systems. In addition to adhering to international data protection and privacy principles in the development of the legal framework, privacy-enhancing technologies and security measures should be built into every aspect of the NIS. Privacy assurance must become an organisational norm.

iii. Individuals must be informed whenever their data is processed, for what purpose, and by which means. The system must be enabled to send transaction notifications and data breach notifications to the data subject.

7.7 Principle 7: Planning for financial and operational sustainability without compromising accessibility

Principle 7 recognises the importance of designing systems that are **financially and operationally sustainable** while still maintaining accessibility for people and reliant parties. This may involve different business models, including reasonable and appropriate service fees for identity verification, offering enhanced or expedited services to users, carefully designed and managed public-private partnerships, recuperating costs through efficiency and productivity gains and reduced leakages, and other funding sources.

Finding and cause: The DHA does not have a defined model to sustain its ID management system through revenue generation.

The following **observations and policy options** apply under the principle:

7.7.1 Financial and operational sustainability

In many cases, particularly where ID authorities report to line ministries, ID systems will be financed out of the national budget. However, digitising ID systems in particular has created the potential for new business models, including generating own revenue by charging fees for identity-related services, as well as public-private partnership models. The following revenue generation streams must be considered:

- Develop policies and a regulatory framework that make provision for revenue generation streams for identification and verification services
- Lower pricing or free services for government agencies
- Market-related fees for the private sector users
- Bulk pricing discounts for frequent users of identity services
- Pricing based on the type of data requested
- Pricing based on whether authentication and verification services are performed online or through hardwired database connection
- Phasing in pricing through initially waiving fees or setting prices extremely low, and later increase them based on demand
- Consider public-private partnerships

7.8 Principle 8: Safeguarding data privacy, security and user rights through a comprehensive legal and regulatory framework

Principle 8 sets out the requirements for a comprehensive legal framework: identity systems must be underpinned by policies, laws and regulations that promote trust in the system, ensure data privacy and security, mitigate abuse such as unauthorised surveillance in violation of due process, and ensure provider accountability. This typically includes an enabling law and regulations for the identity system itself as well as laws and regulations on data protection, digital or e-government, electronic transactions, civil registration, cybersecurity and cybercrime, functional identity systems, etc. The enabling law and regulations for an identity system should clearly describe the purpose of the identity system, the identity system's components, roles and responsibilities of different stakeholders, how and what data is to be collected, liability and recourse for ID holders and reliant parties, the circumstances in which data can be shared, correcting inaccurate data attributes, and how inclusion and non-discrimination will be maintained. Laws and

regulations on data protection and privacy should include oversight from an independent body with appropriate powers and should protect ID holders against inappropriate access and use of their data by third parties for commercial surveillance or profiling without informed consent or legitimate purpose. At the same time, these frameworks should not stifle competition, innovation, or investment and can include regulatory and self-regulatory features.

In addition, the identity-related laws, regulations, and policies should give people genuine choice and control over the use of their data, including the ability to selectively disclose the attributes that they want. Users should be given simple means to have inaccurate data corrected free of charge and to obtain a copy of data held about them. Personal information should not be used for secondary, unconnected purposes without the user's informed consent, unless otherwise required under the law. Identity providers should be transparent about identity management, develop appropriate resources to raise users' awareness of how their data will be used, and provide them with tools to manage their privacy. Identity providers should ensure that the process to correct errors is administrative rather than judicial to increase the speed of resolution and reduce costs. Data sharing arrangements should also be transparent, fully documented, and only agreed to in the best interest of the individual(s) concerned.

7.8.1 Safeguarding data privacy, security

Finding and cause: Legal framework provisions to safeguard data privacy and security have not come into legal effect, leading to personal data being compromised. Some of the provisions of the POPI Act are not yet enforced and the legal framework is currently weak. The ownership, and therefore control, access to and management of the data systems is an issue. The DHA's Information Systems Security Policy is outdated and not aligned to the POPI Act.

The following **observations and policy options** apply under the principle:

i. Government needs to own critical information infrastructure. The technological sovereignty principle must be observed when designing the NIS. That is, the information and communications infrastructure and technology must be aligned to the laws, needs and interests of the country.

ii. NIS must be built on a foundation of trust and accountability between government agencies, individuals, and the private sector, both within countries and across borders. A cornerstone of this foundation are the laws, codes, regulations, and practices that govern and support the ID system, commonly referred to as legal framework.

iii. In general, the policies, laws, and regulations that will support an identity system can be divided into two categories:

- Enablers: directly define and govern the NIS stem, including its design, management, operation, and relationships with stakeholders and other systems.
- Safeguards: address potential risks surrounding the NIS, including those related to data privacy, security, and non-discrimination.

iv. Data dumping to public and private institutions would be discontinued or minimised, and be regulated in accordance with the POPI Act.

v. A legal framework should be established to build trust and accountability in the NIS.

7.8.2 No documented and transparent identity data sharing arrangements between the DHA and identity system users

Finding and cause: There are no documented and transparent guidelines that regulate sharing identity data between the DHA and other ID system users (third parties that have access to either the NPR or Hanis) leading to an unregulated exchange of personal information between parties.

The following **observations and policy options** apply under the principle:

i. Because linking information across databases intensifies privacy and data protection concerns, legal frameworks can mitigate risks by stipulating all the purposes for which personal data in an identity system is shared, by both government and non-government entities. In addition, public and private entities may be limited to obtaining specific information justified by their functions (the "need-to-know" principle).

ii. Personal data collected for other purposes, which could be for an identity system or for civil registration, can be processed by the same or another controller for crime-related purposes only in so far as there is legal authorisation for this and such processing is necessary and proportionate to the purpose for which the personal data was collected.

iii. Disclosure of information, excluding core biometric information, is pursuant to an appropriate court order, which can be made only after the DHA has been given an opportunity to give input on the disclosure. Disclosure of information, including core biometric information, is permitted in the interest of national security on the approval of the director-general or delegated officials.

iv. Personal information about an individual collected for a particular purpose must not be used or disclosed for another purpose without the individual's consent. However, there is an exception for situations where the use or disclosure is reasonably necessary to enforce related activities conducted by, or on behalf of, an enforcement

body. This includes disclosure by police for prevention, detection, investigation, prosecution or punishment of criminal offences, as well as an exception for uses and disclosures authorised by law or by court order. Use for enforcement-related activities must be noted in writing as a mechanism to promote accountability.

7.8.3 User control of identity data

Finding and cause: Sharing personal data of clients occurs without their consent. This arises because some provisions of the POPI Act are not yet implemented.

The following **observations and policy options** apply under the principle:

i. One widely accepted privacy principle is that an individual's personal data should only be collected and used with the consent of that individual unless there is another basis in law for such collection and use. Where consent is the basis for collection, transparent disclosure to the individual of the nature of their personal data collected and the intended uses of such data is essential for consent to be meaningful.

ii. Where the personal data being processed is special category data such as biometric data, additional conditions must be satisfied, one of which is that the individual's explicit consent to the processing should be obtained.

iii. At the point of information collection, consumers must receive notice as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.

iv. Clients must be notified when there are changes effected on their records and identity profiles.

7.8.4 Cybercrime and cybersecurity

Finding and cause: There are risks and weaknesses in the legislative framework that lead to identity theft, such as e-identity theft, and cybercrime. South Africa does not have a comprehensive and effective cybercrime and cybersecurity legislative framework. Legislation on cybercrime and cybersecurity is still a Bill.

The following **observations and policy options** apply under the principle:

i. For each kind of crime in the analogue world, there is an equivalent in the digital world. For instance, theft of property or identity can occur digitally. The occurrences that amount to crime in the real world have a cybercrime parallel in the virtual world. Cybercrime laws provide enforcement powers against such violations.

ii. Cybercrime law should criminalise unauthorised access to the NIS or other databases holding personal data.

iii. Cybercrime law should criminalise unauthorised monitoring/surveillance of the NIS or other databases holding personal data, or unauthorised use of personal data.

iv. Cybercrime law should criminalise unauthorised alteration of data collected or stored as part of the NIS or other databases holding personal data.

v. Cybercrime law should criminalise unauthorised interference with the NIS or other databases holding personal data.

vi. Cybercrime law should clearly state adequate penalties for cybercrime violations, but also for breach of obligations by critical information infrastructure holders.

vii. Cybercrime law should establish clear powers for a computer emergency response teams to prevent and investigate cybersecurity breaches.

7.9 Principle 9: Establishing clear institutional mandates and accountability

Principle 9 highlights the need for institutional mandates and accountability in governing ID systems. Ecosystem-wide trust frameworks must be established and regulate governance arrangements for ID systems. This should include specifying the terms and conditions governing the institutional relations among participating parties, so that the rights and responsibilities of each are clear to all. There should be clear **accountability and transparency** around the roles and responsibilities of identification system providers.

Finding and cause: South Africa does not have legislation that affirms the DHA as the sole provider of official identity services: that is personal data collection, storage and processing. There are other entities outside of government that provide identity verification; however, the DHA cannot challenge these entities as there is no legislation that prevent them from providing this service in any way they see fit..

The following **observations and policy options** apply under the principle:

7.9.1 Clear institutional mandate

- The Home Affairs White Paper alludes to the lack of legislation that declares the DHA the sole provider of identification.
- The legislation must reaffirm and reposition the DHA as the sole provider of official identity and civic status verification services.
- The Home Affairs Bill is part of the process towards a Home Affairs Act to declare, reaffirm and reposition the DHA as the sole provider of official identification.

- The administration of the NIS, including the organisations, staff and procedures involved in its management, operations and oversight, is critical to ensuring that the system is trusted and sustainable.

7.10 Principle 10: Enforcing legal and trust frameworks through independent oversight and adjudicating grievances

Principle 10 emphasises that the identity system should include clear arrangements for the **oversight of these legal and regulatory requirements**. The use of identity systems should be **independently monitored** (for efficiency, transparency, exclusion, misuse, etc.). This will ensure that all stakeholders use identification systems appropriately to fulfil their intended purposes, monitor and respond to potential data breaches, and receive individual complaints or concerns regarding processing personal data. Furthermore, disputes regarding identification and personal data use that are not satisfactorily resolved by the providers – for example a refusal to register a person or to correct data, or an unfavourable determination of a person's legal status – should be subject to a rapid and low-cost review by independent administrative and judicial authorities with the authority to provide suitable redress.

Finding and cause: There is no independent oversight for the identity management system and some of the provisions of the POPI Act have not yet come into effect.

The following **observations and policy options** apply under the principle:

i. To ensure compliance with privacy and data protection laws, the following options are recommended:

   - The **Information Regulator** (South Africa) could be declared an independent oversight authority to monitor the use of official identity information.
   - Establish an independent body that is legally empowered and has the capacity to oversee official identity processing and to hold responsible parties accountable.
   - Establish a semi or fully autonomous agency or directorate within the DHA that is legally empowered and has the capacity to oversee official identity processing and hold responsible parties accountable.

SECTION D: ENVISIONED IDENTITY MANAGEMENT SYSTEM

Chapter 8: Key elements of the identity management system

8.1 Introduction

The identity management system consists of the following key elements:

- Single digital population register of all people who live and have lived in the country
- Biometric-based NIS that enables a single view of a person, e-government and e-commerce
- Policy that provides for a constitutionally sound framework to manage personal information that will be collected and stored in the NIS
- Legislation that establishes clear rules to govern accessing and processing the population register records in line with relevant policies and legislation such as the POPI Act and Cybercrimes Bill.

The DHA can only carry out its constitutional commitments if it is the sole custodian of the official identity of all citizens and all persons in South Africa. In a digital age, this requires building a population register that can affirm, secure and verify e-identity corresponding to the register of identity of natural persons.

8.2 The new population register

The new population register will incorporate the civil registration of citizens, data from the immigration system and aspects of the current population register. Each item included in the population register will be specified in a new Population Register Act. In a digital age that is data-dependent, the data specified in the Act will have major implications for citizens, the State and the economy.

The population register, as conceptualised in the White Paper and supported by the NIS, is an instrument that the State will use to keep and process legally specified records and data on every citizen and every person in South Africa. It will be a central feature of a digital society and globalised economy, and the backbone of e-government. To play this role, population register records and data must be digital, accurate, current and secure. This, in turn, depends on establishing enablers to ensure that the systems producing the

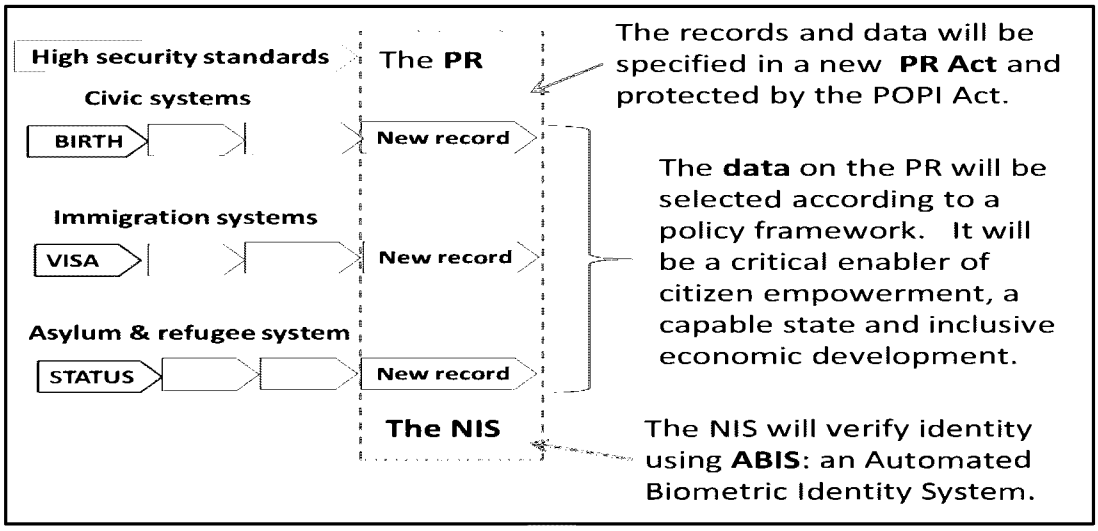
records have a firm policy and legal foundation, with up-to-date technology. They must operate within an environment that is secure and well-governed.

The argument for South Africa to invest in the kind of population register outlined above is made in the 2017 version of the Mandate Paper, published annually by the DPME as a guide to government budgeting approaches and priorities:

> *Improved operational and information systems will help fight crime and corruption but also government efficiency generally. Ongoing technological change is driving down the cost of effective administrative, information and monitoring systems. A bedrock of such administrative systems is an effective identity system for citizens and visitors. It is therefore critical to ensure that the population register of the Department of Home Affairs and the electronic and card Identification system include all citizens and be of the highest integrity. Obstacles to a more rapid rollout must be investigated and a comprehensive integrated approach developed about how this system can be integrated with other government programmes and systems. (The views expressed above were elaborated in the 2018 Mandate Paper).*

The basic model of the NIS as demonstrated in Figure 8.1 shows how the model will work. The civic, immigration and refugee systems have outputs that result in creating a new or updated record. In the examples, these would respectively be a birth certificate; a visa such as a tourist, work or study visa; and a decision to grant or deny refugee status to an asylum seeker. The population register is part of the same digital platform and is the database where the records and data specified in a Population Register Act reside. The integrity of the population register depends on the integrity of all the systems, which must meet high standards of security as specified in relevant Acts and produce data that is accurate and reliable.

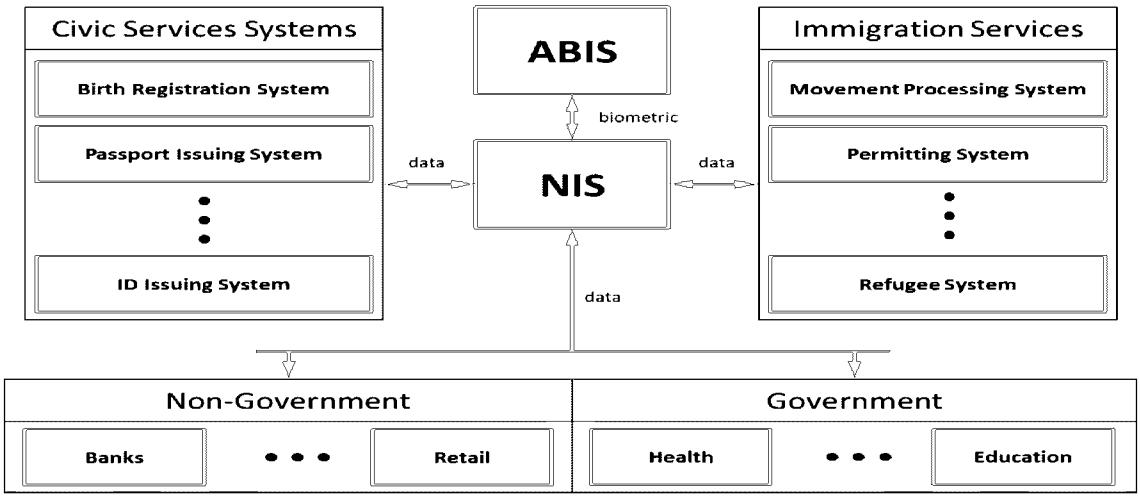
Figure 8.1: The new population register supported by a National Identity System



8.3 The envisaged NIS

The NIS will be an integrated system built around a multi-modal Abis. The NIS will support identification searches to establish the identity of a person with a given biometric, and verification searches to confirm whether the identity document belongs to the person whose biometric is presented. It will be scalable and expandable to include additional biometrics such as iris scans, palm prints and footprint and facial recognition. Figure 8.2 illustrates how such an interface will be enabled.

Figure 8.2: NIS interface platform



The NIS will be developed in phases based on open standards to ensure seamless integration of all government IT systems. All modules will be developed as required and will be based on the functional and technical specifications that are based on re-engineered business processes. Developing the NIS modules will be fully implemented once the information from the legacy systems (NPR, Hanis, EMCS and NIIS) have been cleaned up. Every case requiring data clean-up should be tracked through a case management system to investigate and report on the nature of challenges encountered and progress made towards resolution of the cases detected.

The NIS is the envisaged single source of all DHA client data. It will consolidate the data stored on the NPR, NIIS, MCS, EMCS, VAS and the visa system into one database. The NIS will serve as the link between other systems and Abis; i.e., insertion of and access to the biometric data stored on Abis will be through the NIS. The NIS has the following objectives:

i. Record the department's interactions with clients (i.e. travellers and all persons that are resident in South Africa).

ii. Ensure accuracy and integrity of the client data.

iii. Ensure that all client records are linked uniquely to each client.

iv. Record all changes to a client record and store historical data.

v. Link all transactions (data insertions, data requests, and data updates) to DHA officials who perform the transaction in such a manner that the official who performed the transaction cannot dispute the transaction.

vi. Provide interfaces for systems of organisations outside the DHA to access client data.

vii. Ensure that data stored in the NIS is available in real time.

The main function of the NIS will be to ensure the storage and integrity of client data. All data that is concerned with the identity of a DHA client, citizen and non-citizen, will reside in the NIS. The DHA's business processes will be executed in front-end systems, such as Live Capture, and the NIS will only store the data generated from those front-end systems. The NIS will provide access to its data via a catalogue of services, which in turn will be used by the interfacing systems to perform their functions. The services that the NIS will provide can be broadly grouped as follows:

i. Query: all interactions where data residing in the NIS is only being retrieved; i.e., the data from the NIS is merely used to accomplish some desired function, but remains unchanged after the interaction. This is inclusive of verification and identification, which entail more than the simple retrieval of data.

ii. Modify: all interactions where data residing in the NIS is only being updated or changed from its current value.

iii. Create: all interactions resulting in the genesis of a new record. Once a record is created, all subsequent interactions with it will be modify interactions.

iv. Insert: this is not a fundamental interaction type of the NIS but it is used to represent all interactions involving new information being entered into the NIS. This consists of both modify and create interactions.

v. Retrieve: this is not a fundamental interaction type of the NIS, but it is used represent all interactions involving existing information being requested from the NIS.

vi. Push: this involves the automatic propagation of data from the NIS to any of its interfacing systems. Push services provide the capability to send data to external systems without necessarily being initiated by an external system to the NIS. These services are typically initiated when specific "trigger" events occur within the NIS, where it has been determined that an external system should be updated automatically upon occurrence. An example of this is when the NIS receives information about a v-listed individual. The NIS in turn will automatically push this information to relevant systems such as the risk engine, so that it too has the latest and most accurate version of the v-list.

vii. Deactivate: this is an interaction whereby the data of a record or the record itself is removed from the active set of the NIS and placed in an inactive set, which is only accessible with the requisite authorisation.

Given the pivotal nature of the NIS to the operations of the State and society, and the sensitive nature of the personal information contained in it, proper privacy and security measures will be put in place to protect it from unauthorised modification and external tampering or hacking. Key security measures will include biometric access control including non-repudiation measures for officials and audit logging of any transaction processed on the NIS. The NIS will also ensure the secure issuance of enabling documents to eligible applicants. Key enabling documents will be secured by including security features. The introduction of the smart ID card and the new secure passport (an ICAO-compliant machine-readable travel document) are part of the security improvements that form part of the NIS rollout.

All access to digital data and records will be rule-based and governed by appropriate legislation. Rules that ensure security and the rights of citizens and residents will derive from cyber security and privacy legislation. The new population register will be comprised of legally mandated records that are accurate, highly secure and linked to biometric data that relates to a unique individual. It will be the basis of a trusted official e-identity that will be the backbone of the digital platforms, State and private, that all our lives will depend on. The population register will enable all communities to access responsive and integrated digital services and information. The following security components are needed for the NIS:

i. Identity and access management refers to the processes and tools used to grant or deny access and authorisation to the NIS. It will be realised by the following services: identity management, access control services, authentication services and privilege usage management service.

ii. Data governance refers to management and control of data to ensure that high-quality data exists within the NIS over the lifecycle of the data.

iii. Data security and privacy ensures that policies, procedures, functions and tools are provided to classify data and protect it from unauthorised disclosure, modification, theft and leakage.

iv. Threat and vulnerability management refers to the continuous or cyclic practice of monitoring, identifying, classifying, remediating, and mitigating of system security weaknesses.

v. Secure infrastructure hardening ensures that all the NIS infrastructure components, and the associated software and platforms for both, are continuously secured.

vi. Centralised logging ensures that all the activities such as user access, transactions, user permissions, transaction patterns, etc. are stored centrally and that the storage is protected from any modifications by either authorised or unauthorised users of the NIS.

vii. Business continuity / disaster recovery refers to the policies, procedures, facilities, tools and functions that ensure that there will be no loss of NIS data following a disaster of any kind.

viii. Information security governance refers to the tools, policies, personnel and business processes that ensure that security is continuously carried out to meet NIS-specific needs in line with relevant legal and regulatory frameworks.

ix. Risk analysis and management refers to the tools and processes needed for identification, analysis, monitoring and mitigating system risks during the lifecycle of the NIS.

x. Device management refers to securing (such as securing file systems) of all devices that connect to the NIS to avoid tampering with these devices.

Further modernisation and integration of systems mean the DHA must introduce Abis, which will enable further biometrics capturing. The Abis project will be rolled out in phases, over a five-year period. Among others, implementation will entail migration of the current Hanis data (fingerprints and facial recognition) to the new Abis, with improved functionality, installation and configuration of Abis infrastructure (hardware), and building system functionalities. The current Hanis only records two biometrics; that is, photos and fingerprints. Abis will record at least five biometrics; that is, fingerprints, palmprint, facial, iris and photo recognition. It is envisaged that, in future, the DNA and child footprint will be added to Abis.

Chapter 9: Legislative framework

The White Paper contends that the DHA rules that govern access to, and processing of, population register records and data, including verifying identity, will be based on a new legislation, regulations and operating procedures. The legislation will replace the current Identification Act that dates back to the 1980s, although it was deracialised post-1994. The new legislation will specify the mandatory records and data that must be in the population register, according to a policy and legislative framework aligned to the Constitution of a sovereign, democratic South Africa.

The current Identification Act establishes a population register and specifies its scope in the mandatory records that are captured on it. In terms of categories of persons, the current population register covers all South Africans, including those residing abroad, and foreign nationals who are permanent residents. The Identification Act also covers the biometric and biographical data captured on the population register and the specifications of the identity documents that are issued.

The Identification Act's objectives specifically include (among other things) compiling and maintaining a database in respect of the population of the Republic of South Africa and the issuing identity cards, birth certificates, marriage certificates, death certificates or passports to persons whose details are included in the database. The director-general of the DHA, according to section 5 of the Identification Act, is responsible for ensuring that:

- the database is compiled and maintained
- the particulars required for compiling and maintaining the database are obtained, in accordance with the provisions of the Identification Act.

The Identification Act only refers to the population register and does not distinguish between the underlying systems or their purposes. The population register is implemented through the following systems:

- the NPR managing biographical information
- Hanis managing biometric information, notably fingerprints, facial photographs and signatures.

The new legislation will provide for the following key policy changes:

i. Provisions that reaffirm the DHA as the sole provider of official identity services; that is, collection, storage and processing of personal data (biographic and biometric data).

ii. Provisions for the establishing the population register as the only official record or database for all people who live or lived in the country.

iii. Provisions for collecting new biometrics such as iris scans, palmprints and footprints and facial recognition.

iv. Provisions for collecting, storage and processing official identity data for all people (citizens and non-citizens) who live/lived in the country, or international visitors.

v. Provisions for collecting storage and processing official identity data for people that are currently discriminated against on the basis of their sex.

vi. Provision for registering all births (citizens and non-citizens) in the population register.

vii. Provisions for capturing biometrics of children at birth or, where impossible, biometrics of a parent or informant.

viii. Provisions for reconfiguring the ID number to accommodate excluded minority groups, including intersex persons.

ix. Provisions for establishing a single digital NIS that enables a single view of a person, e-government and e-commerce.

x. Provisions for securely sharing official identity data with public and private institutions in line with the POPI Act and Constitution (realisation of the privacy principle).

xi. Provisions for establishing an institutional capacity for independent oversight of the NIS and processing personal data.

xii. Provisions for hefty penalties for those who aid identity fraud and theft, and illegal processing of personal data (including amendments to personal data without the consent of the affected person). This should also cover cybercrimes.

xiii. Provisions for criminalising burying a person without a death certificate that is issued by a relevant authority.

Other legislation that will be amended include the following:

- Births and Deaths Registration Act 51 of 1992
- Regulations made under the Births and Deaths Registration Act 51 of 1992
- Regulations made under the Identification Act 1997
- Alteration of Sex Description and Sex Status Act 49 of 2003.

The South African population register will be among the most integrated, comprehensive and connected systems globally, with significant benefits for the State, the economy and

citizens. The centrality of data in a digital world will mean enabling legislation that aligns with Acts dealing with areas that include privacy, copyright, cyber security, national statistics, archives and records. Population register records will eventually need to be archived indefinitely for two main reasons: to preserve a record of who constituted the nation for future generations and as a database that is a crucial resource in a digital knowledge-driven society.

Chapter 10: Funding model

The DHA's budget of just R8 billion (2019-20 financial year, inclusive of the IEC transfers) is based on the incorrect assumption that it does not require modern systems, professional staff and a secure environment. The consequences of the funding deficits have been very costly for South Africa, leading to deprivation of constitutional rights to citizens and eligible non-citizens. This has also contributed to the increase of illegal migration since the inspectorate capacity and budget have shrunk over the years. A secure, modernised DHA that is funded at an appropriate level by the State would be a key enabler of economic development and would generate new revenue streams and investments.

Given the fiscal pressures, it will be impossible for the State to fully fund the repositioning programme. The project for a detailed design and cost projection of the new model DHA will be launched in the 2020/2021 financial year.

Other (current and future) revenue streams:

- Tariffs for civic and immigration services: this revenue stream is current but tariffs remain very low especially for passports, visas and permits.
- Self-financing (revenue collected through the tariffs is returned from the NRF to DHA): this revenue stream is current; however, it is dependent on the National Treasury approval.
- Charges for verification of identity and status in official transactions: this revenue stream is current but the automated billing system is not operational (manual invoicing is being used).
- Charges for verification of identity and status in commercial transactions: this revenue stream is current but the automated billing system is not operational (manual invoicing is being used).
- Additional charges for premium services: this revenue stream is at a conceptualisation stage.
- Fees for interfaces with the NIS: this revenue stream is at a conceptualisation stage.
- The successful implementation of the NIS will lead to a substantial reduction in fraudulent transactions across the State and society. The reduction in social grant fraud alone will more than pay for its development over the medium term; new revenue streams could be generated; and many forms of partnerships developed.
- As part of removing barriers for accessing DHA services, the department will

develop an indigent policy to cater for the poor who are not able to pay for reissued mandatory enabling documents. This will include first-time applicants for smart ID cards who already have green ID books.

SECTION E: IMPLEMENTATION STRATEGY AND ROADMAP

Chapter 11: Phased-implementation approach

The identity management system will be planned according to the following horizons:

- Three-year horizon (April 2019 – March 2022): The focus is on putting in place the policy and legal framework for the population pegister and NIS.
- Five-year horizon (by March 2024): All core elements of the new population register and NIS are fully functional, including basic administrative and core business systems, and required security standards are maintained. That is,
    - integration of DHA systems completed
    - the NIS interfaces with critical government systems
    - a single database for government and e-government platform is operational
    - the NIS interfaces with private sector systems
    - the NIS interfaces with systems of neighbouring countries – piloted through the one-stop border post initiative
    - The population register is generating substantial revenue through large-scale verification of identity.
- Ten-year horizon (by March 2029): The envisioned end-state is achieved with the legacy model fully replaced, world-class standards maintained and funding assured.

The department is undertaking deep-dive studies that will enable the development of clear and realistic implementation strategies. The focus areas include:

Human resources management and development:

- The new model DHA requires officials who understand policy, law and processes and can investigate and solve problems while securing systems under constant threat from criminal syndicates. As a result, the recruitment and training of an employee that is security aware is critical to establishing the kind of secure environment needed.
- The DHA will not be able to reposition to a secure and modern department with the current competences of its employees. It is envisaged that the results of the study will determine the readiness of the department and will further enable the DHA to take firmer control of key functional areas in preparation for a

comprehensive implementation of the repositioning programme. The strategy is to capacitate the Learning Academy as a college that will help the department to retrain employees for a repositioned DHA

Information communication technology

- The current repositioning programme is the most critical factor in transforming the DHA as a modern and secure department and an integral part of the security apparatus of a capable State. The DHA vision for its systems is to build one integrated digital platform with a single NIS at its centre that serves both civic and immigration functions and enable a single view of a person. Such a platform requires a new operating model, with highly trained officials guided by appropriate values and legislation within a secure environment.

- It is imperative that a diagnostic study be conducted to assess the state of ICT in the department as this is one of the critical enablers of successfully implementing the repositioning programme. It is envisaged that the results of the study will determine the readiness of the department and outline all the necessary measures that need to be put in place prior to implementing the repositioning programme.

Security and enforcement

- In executing its mandate, the DHA plays a very critical role in protecting the integrity of the country as a sovereign State through securing and managing the official identity and status, international migration, refugee protection and population register. As it is, the DHA will not be able to reposition to a secure and modern department with the current security and enforcement capacity.

- With the DHA being repositioned as a modern, secure department located within the security system of the State, there is a need to enhance its capability to mitigate risks, deal with threats and respond to national security demands. This requires building and maintaining a security system around its people, systems, data and infrastructure. Therefore, prior to the DHA embarking on the actual implementation of the repositioning programme, an organisational assessment of the security and enforcement capabilities will be undertaken through a deep-dive study.

- It is envisaged that the results of the study will determine the readiness of the department and will further enable the DHA to take firmer control of key functional areas in preparation for a comprehensive implementation of the repositioning programme.

Funding/revenue generation model

- One of the key arguments for repositioning is that financial constraints are preventing the DHA from continuing with its transformation and threatens to undermine the progress it has made thus far.
- Although the DHA is a critical enabler of citizen empowerment, inclusive development, efficient administration and national security, it is currently not fully funded to deliver its mandate efficiently while its mandatory services to the public remain the same.
- A secure, modernised DHA that is funded at an appropriate level would be a key enabler of economic development and would generate new revenue streams and investments. To address this gap, an appropriate funding model for the DHA is of necessity and will contribute to ensuring that the DHA reposition itself to fulfil its vision of being a fully modernised and secure department, with professional staff and appropriate operating, organisational and funding models. There is a clear need for a new funding model for a repositioned DHA that is located within the security of the State.

It is envisaged that the deep-dive studies will be finalised during the 2020/2021 financial year, and they will enable the finalisation of a detailed (short-, medium- and long-term) implementation plans for repositioning the department; this includes the full operation of the population register and the NIS.

The department is in the process of establishing a programme management office (PMO) that will oversee the implementation of the repositioning programme. The strategic vision of the DHA PMO remains "A programme management office that is internally institutionalised and positioned as a catalyst to successfully deliver special projects of the department. DHA PMO strategic mission is to provide a solid foundation for the projects of the Department of Home Affairs by creating an environment of measurable, disciplined project management professionalism."

Change management and communications are core elements of the repositioning programme. The shape of the repositioned DHA will inevitably be different; and will require an extensive change management programme over seven to 10 years.

The change management directorate has developed a change management strategy that includes the following elements:

- Awareness campaign on the repositioning programme
- Appointment of youth as change agents for the repositioning programme
- Appointment of senior managers as champions for the repositioning programme

- Training change agents on the repositioning programme and its implications for employees
- Preparation for a future-fit DHA.

DEPARTMENT OF HOME AFFAIRS

NO. 1426 **31 DECEMBER 2020**

MINISTRY
HOME AFFAIRS
REPUBLIC OF SOUTH AFRICA

Private Bag X741, Pretoria, 0001 Tel: (012)432 6600 Fax: (012) 432 6637
Private Bag X9102, Cape Town, 8000 Tel: (021) 469 1600 Fax: (021) 461 4191

ONE-STOP BORDER POST POLICY

I, Dr Pakishe Aaron Motsoaledi, Minister of Home Affairs, intend in terms of section 85, sub-section 2 (b) of the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996) to publish the One-Stop Border Post policy for public comments.

Interested persons and organisations are invited to submit any substantiated comments or representation by no later than 28 February 2021. Written submissions can be forwarded to the following address:

The Director-General: Department of Home Affairs, Private Bag x114, Pretoria, 0001

For attention: Mr Sihle Mthiyane, Chief Director: Policy & Strategic Management

Or via email: osbppolicy@dha.gov.za

Tel: 012 406 4353

DR PA MOTSOALEDI, MP
MINISTER OF HOME AFFAIRS
DATE: 29/12/2020

Department:
Home Affairs
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF HOME AFFAIRS

DRAFT ONE-STOP BORDER POST POLICY

PUBLIC CONSULTATION VERSION

22 DECEMBER 2020

Contents

Definitions

Border law enforcement	The execution and enforcement of legislation relevant to facilitating and managing the legitimate movement of goods and persons within the border law enforcement area and ports of entry
Border law enforcement legislation	All relevant legislation dealing with border law enforcement
Cluster	Administrative unit formed by government departments to facilitate coordination, planning and delivery
Commercial port of entry	A location where infrastructure, systems and staff are in place to facilitate the entry and exit of commercial goods and vehicles through a port of entry
Common control zone	Clearance formalities for goods, people and means of transport exiting one country and entering another are usually conducted in a shared space, where border officers of adjoining countries are entitled to apply their respective national laws
Constitution	The Constitution of the Republic of South Africa, 1996
Conveyance	A system or means of transporting people or goods
Cross- border agents	Facilitates trade and, in some countries, are an essential part of the cross-border movement systems for goods and conveyances
Criminal law	The body of law that defines criminal offences, regulates the apprehension, charging and trial of suspected persons, and fixes penalties and modes of treatment applicable to convicted offenders
Electronic single window system	One of the international standards or good/best practice that enables cross-border traders to submit relevant documents at a single location and/or through a single entity
Exclusive zone	Refers to a facility or an area designated within the common control zone of the host partner State for the respective exclusive use and access by border officials of the adjoining partner States to execute border controls and related matters
Extraterritorial jurisdiction	Application of national jurisdiction in another country that is enabled by a bilateral agreement or international agreement
Facilitation	Procedures used by a State to enable people, goods or conveyances to legally transit across an international border
Jurisdiction	The right, power, or authority granted to a legal entity to administer justice or perform a function
One-stop border concept	Refers to the legal and institutional framework, facilities and associated procedures that enable goods, people and vehicles to stop at a single facility for the necessary checks and controls, following

	applicable regional and national laws, to exit one State and enter an adjoining State
One-stop border post	A land port of entry where two countries cooperate to enable a single and harmonised clearance of people, goods and conveyances
Partner state	A sovereign State that is party to a border agreement
Port of entry	A port of entry designated by the minister in terms of section 9A of the Immigration Act 13 of 2002 and includes any port, point or place of entry or exit determined under any other legislation or any other port, point or place of entry or exit approved by the minister in terms of section 30 of this Act
Preclearance	Critical processing that enables importers and exporters to submit trade documents to border agencies prior to the arrival of goods at a point of clearance
Single window system	Lodging standardised information and documents at one point to fulfil facilitation requirements for people, goods and conveyances
Trade corridor	In the context of one-stop border posts, the route by which most freight travels before, through and after the border, and continues to its destination
Traditional two-stop boarder post	Exit procedures are carried out on one side of the border for persons, vehicles and goods leaving a country

Acronyms

4IR	Fourth Industrial Revolution
APEC	Asian Pacific Economic Cooperation
AU	African Union
BLE	Border law enforcement
BMA	Border Management Authority (previously Agency)
CBRTA	Cross-Border Road Transport Agency
CCZ	Common control zone
DAFF	Department of Agriculture, Forestry and Fisheries
DHA	Department of Homc Affairs
EAC	East African Community
GDP	Gross domestic product
HR	Human resources
ICT	Information and communications technology
IMF	International Monetary Fund
JICA	Japan International Cooperation Agency
OCAS	Operator Compliance Certification Scheme
OSBP	One-stop border post
PoE	Port of entry
POPIA	Protection of Private Information Act
RKC	Revised Kyoto Convention
SA	South Africa
SADC	Southern African Devclopment Community
SANDF	South African National Defcnce Force
SAPS	South African Police Service
Sars	South African Revenue Service
TWG	Technical Working Group
WTO	World Trade Organization

SECTION A: BACKGROUND AND CONTEXT

Chapter 1: Overview of the South African border environment

1.1 Introduction

As a sovereign constitutional State, South Africa's land border is recognised by its six neighbouring States: Botswana, Eswatini, Lesotho, Mozambique, Namibia and Zimbabwe. As independent countries, each of these States have laws that apply within their territories, which includes the right to decide what goods, conveyances and persons enter or leave their territory. States have a right to protect their territory, resources and people from natural or human risks and threats, and to make decisions in their national interest.

States must therefore enter into agreements to establish designated ports of entry (PoEs) where officials of both States use laws, procedures and systems to control and facilitate the flow of traffic, which includes people, goods and conveyances. It is in the interest of both countries for the process at a PoE to be secure, efficient and aligned to their development goals.

The Immigration Act 13 of 2002 gives the minister of home affairs the authority to designate a PoE as the point at which people, conveyances and goods may legally enter and exit South Africa. South Africa currently has 72 such PoEs.

Table 1.1 is a list of South Africa's 72 PoEs and their status as land, sea or air ports.

Table 1.1: South Africa's border profile (2018/2019)

Designated land ports	53
Designated sea ports	8
Designated international airports	11
Designated PoEs	72
Registered small airfields	150
SA coastal borderline	3 924 km
SA land borderline	4 471 km

South Africa has seven cross-border rail crossings, which are primarily used for commercial goods and occasionally for passenger rail, and co-manages six trans-frontier conservation national parks with her neighbours.

South Africa's land, sea and air borderlines are presently safeguarded by the South African National Defence Force (SANDF). When the Border Management Authority (BMA) assumes border law enforcement functions within the land and maritime border law enforcement areas

(or borderlines) between PoEs, the SANDF will simultaneously perform border protection functions in these areas.

South Africa's PoEs have representatives from five organs of state to enforce border law and ensure that traffic is regulated through these ports.

A further 10 organs of state are involved in managing aspects of the larger border environment. South Africa is committed to establishing a border environment that is managed in a way that is integrated, secure and efficient. This national one-stop border post (OSBP) policy is an important enabler in achieving this policy goal.

1.2 Border environment

The concept of a **border environment** encompasses the borderline, the PoEs and the context in which they are situated: environmental, social, legal, transport, economic and political.

In many instances, communities along the border have been divided by borderlines. However, the communities themselves have continued their ties dating back many years. These communities are mostly located along Lesotho, Eswatini, Mozambique and parts of the Botswana borderline. Examples of PoEs with informal border crossings include Gate 6, which is situated along the borderline between South Africa and Mozambique, and the pilot community border crossing point located at Tshidilamolomo in the North West, which borders Botswana.

There are many role players involved in the border environment and at PoEs, with local government officials, communities, workers and businesses all located near the ports. For example, Lebombo is a land PoE located on a major trade corridor with many ties between the towns on either side of the border. The towns are economically dependent on traffic from a port or industrial zone hundreds of kilometres away. Lebombo therefore has officials responsible for immigration, customs, policing, health, biosecurity and phytosanitary controls. All public transportation vehicles have to pre-clear their routes, passengers and goods with the Cross-Border Road Transport Agency (CBRTA), which operates outside of the PoE, and must comply with certain standards. Therefore, a truck with cattle from Mozambique destined for an auction in South Africa will have been cleared by customs, Department of Agriculture, Forestry and Fisheries officials, and CBRTA officials. A freight forwarding agent may also have been involved in the transaction and the driver would have been cleared by an immigration officer. The health official may inspect travellers for any threat to public health. Such processes involve applying both domestic and international laws and agreements that have been ratified by the two respective countries.

The SANDF is responsible for the borderline and should be informed, for example, of smuggling activities across the borderline or if persons are suspected of crossing the border illegally. The Department of Public Works and Infrastructure maintains infrastructure such as roads and fences. The Department of Transport monitors road use and works with the South

African Police Service (SAPS) and other departments to prevent overloaded trucks or buses having accidents and damaging the road.

Those officials from the 22 departments and agencies that are active in the South African border environment who frequently work within the PoE have regular meetings with other officials rendering their services at the PoE. The meetings serve to manage risks, combat crime and improve services and efficiency. All these officials must comply with laws and regulations, and relevant priorities and targets set out in national, provincial and local government programmes and plans. They will face foreseen pressures such as traffic flows increasing in peak seasons, and unforeseen pressures such as a flood or an outbreak of a disease that has an impact on humans, plants or animals. Officials must also respond to issues raised formally and informally by their counterparts at various levels in neighbouring countries.

Departments and local government in the border environment must manage complexities that include mixed flows of migrants such as asylum seekers and work seekers, flows of private and commercial vehicles, and travellers on foot. Officials from local municipalities and provincial government also frequently interact with PoEs regarding the services required by, and the impact of local activities on, the port. Apart from standard municipal services, local government must provide specialist services such as finding shelter for abandoned children. Local government also has constitutional obligations such as providing basic healthcare and security for all persons.

In addition to the immediate border environment, every commercial PoE is organically connected to the interior of at least two countries through the transport and trade corridors in which they are situated. A strike at the docks in Durban affects the Lebombo PoE and vice versa. Delays in clearing commercial vehicles at a PoE disrupts the flow of trade on both sides of the border and along a network of corridors stretching over southern Africa and beyond. Delays at any PoE have a negative impact on local traders and business, and on the tourism industry of two or more countries.

This logistical network and South Africa's comparatively advanced transport and economic infrastructure attract both legitimate trade and investment, and local and transnational criminal syndicates. The same syndicates may be involved in smuggling and trafficking people, endangered species, arms, drugs and/or contraband. They are involved in corruption, money laundering and fraud, including immigration and tax fraud. Some of the money generated by cross-border crime may be used to fund terrorism or criminal activity anywhere in the world. Information provided by the systems operating at PoEs is essential to national security and combatting crime, and for national statistics used in planning and making strategic decisions.

1.3 Border management risks and challenges

The salient border management risks and challenges facing South Africa can be summarised as follows:

- The South African border environment is characterised by poor controls and weak management that adversely affect its territorial integrity.
- South Africa has an extensive and geographically diverse land border environment that is shared with six neighbouring countries. The geographic implications of South Africa's land border environment are that border safeguarding and control activities are required in a variety of environments ranging from mountainous to semi-desert areas.
- Border infrastructure, such as fences and patrol roads, are inadequate. The capability of the State to secure this environment is limited and exposes large parts of the land border environment to strategic vulnerability, which contributes to problems such as wildlife poaching, human trafficking and smuggling.
- The location, number and design of South Africa's 72 PoEs are a legacy of the country's colonial and apartheid past. Key challenges include the uneven provision of border control services to travellers and traders, embedded corruption, insufficient deployment and use of human and technological resources, and fragmented border management.
- The fragmented model of coordinated border management in South Africa has failed. This approach to border management has contributed to significant imbalances and discrepancies in security, managing border risk, uneven remuneration and conditions of service for border control officials, and a silo approach to service delivery by individual organs of state.

1.4 Towards an integrated border management approach

Since 1994, South Africa has made great strides in strengthening how it manages the country's borders by introducing various capabilities to give effect to border management. Structures to coordinate the mandates and actions of distinct organs of state in the border environment included the following:

- Border Affairs Committee Coordinating Committee (1996)
- National Inter-Departmental Structure (1997)
- Border Control Operational Coordinating Committee (2001)
- Inter-Agency Clearing Forum (2010)

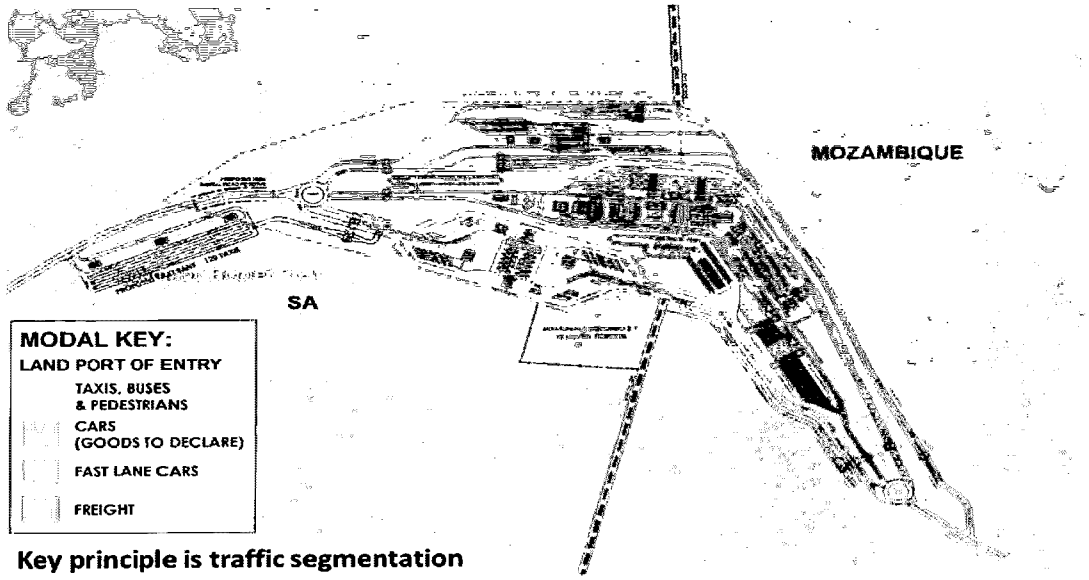
Despite these efforts, a silo and fragmented approach to border management, border law enforcement and border protection has persisted. Since the mid-2000, various studies and reports pointed to the failure of these structures to address the systemic and structural problems of the coordination model associated with fragmented border management. It is against this background that, on 26 June 2013, Cabinet resolved to establish a BMA in South Africa. The

BMA will be outcomes focused, balancing facilitation of legitimate trade and travel functions with addressing security risks for South Africa. The BMA will introduce a more streamlined, secure and efficient way of managing South Africa's borders. It will follow an integrated border management approach for secure and effective borders that will better support the National Development Plan, the Medium Term Strategic Framework and South Africa's economic development priorities.

The BMA, together with the South African Revenue Service (Sars), will in future play a valuable role in improving governance, security and efficiency at PoEs. The BMA will therefore be at the forefront of fighting illicit and unauthorised movements of goods and people through South Africa's ports. Port health services will integrate with the BMA, giving it the ability to seamlessly and rapidly mobilise additional border law enforcement capability from within the BMA. The BMA will be established as a national public entity and will report to the minister of home affairs.

The Department of Home Affairs (DHA) is also redeveloping six land PoEs. This major project is aimed at modernising the Beit Bridge, Lebombo, Oshoek, Kopfontein, Maseru Bridge and Ficksburg PoEs into world-class OSBPs. The construction of these PoEs as OSBPs is expected to be complete by 2025. The benefit for the South African economy is that goods and people will move through these six busiest land ports at a faster pace and in a more effective and efficient manner. This will have specific and direct economic benefits for traders, freight carriers and all those transporting goods since the intention is that all movement through these ports will be processed once and jointly between South Africa and the relevant neighbouring country. The master plan of the Lebombo OSBP is presented below to demonstrate the envisaged design of the OSBPs.

Figure 1.1: Lebombo OSBP master plan



Chapter 2: The strategic role of PoEs

2.1 The corridor perspective

Trucks, trains, buses and other conveyances move people and freight in both directions along transport corridors, connecting them to land, sea and air ports and centres of production and consumption. Transport corridors that cross two or more countries enable them to trade with one another and with the rest of the world. They also serve a range of other needs, including the delivery of services and the movement of migrant workers and tourists. When this stream of traffic flows through a land border post, it can act as a choke point if the movement is not facilitated quickly, efficiently and effectively, causing costly delays and disrupting economic and social activities.

The concept of a trade corridor[1] refers to the streams of products, services and information that flow into and along transnational trade routes, enabled by domestic and international law, agreements, institutions and systems. From this viewpoint, a land border post is a stage in a process that begins with the facilitation of a shipment for export before it leaves a factory, its clearance at a PoE and the steps it goes through to reach its destination to complete the cycle, such as acknowledging receipt and paying any taxes or fees due.

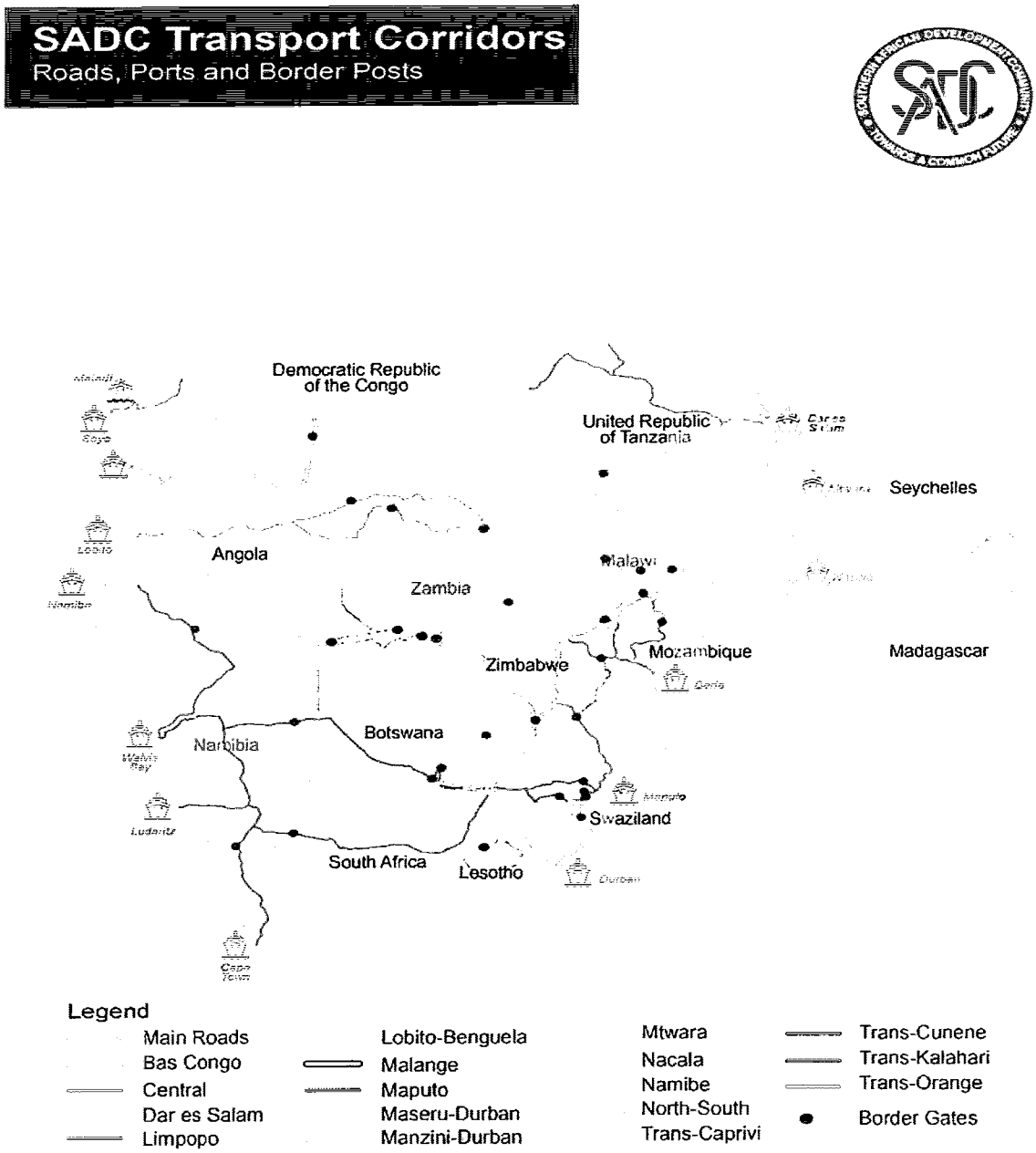
To realise the value of the OSBP methodology, it must be applied at both the transport and trade corridor levels. Steps must be taken to ensure more efficient facilitation within the border post environment, and to simplify and harmonise relevant processes and procedures at the level of the legislation and systems of two or more countries. This is an ongoing process, with minimum requirements, phased development and the need to respond to changing technology and circumstances.

South Africa's corridor networks connect the region internally, to the rest of Africa and to the world. The efficacy of the entire transport and trade system depends significantly on the effective and efficient facilitation of traffic through PoEs.

Figure 2.1 provides a map of South Africa's transport and trade corridors. The north-south corridor links the Port of Durban with Central Africa and connects with the Dar es Salaam corridor in Tanzania. This corridor network connects 26 countries, which explains why Beit Bridge, on the border with Zimbabwe, is South Africa's largest land border post in terms of volumes and value of traffic. This is followed by Lebombo on the Maputo corridor, which connects South Africa to the Port of Maputo in Mozambique. The trans-Kalahari and trans-Caprivi corridors connect Namibia with Gauteng, which is South Africa's economic hub, and the trans-Cunene corridor connects Namibia to Angola.

[1] Sometimes termed logistics corridor

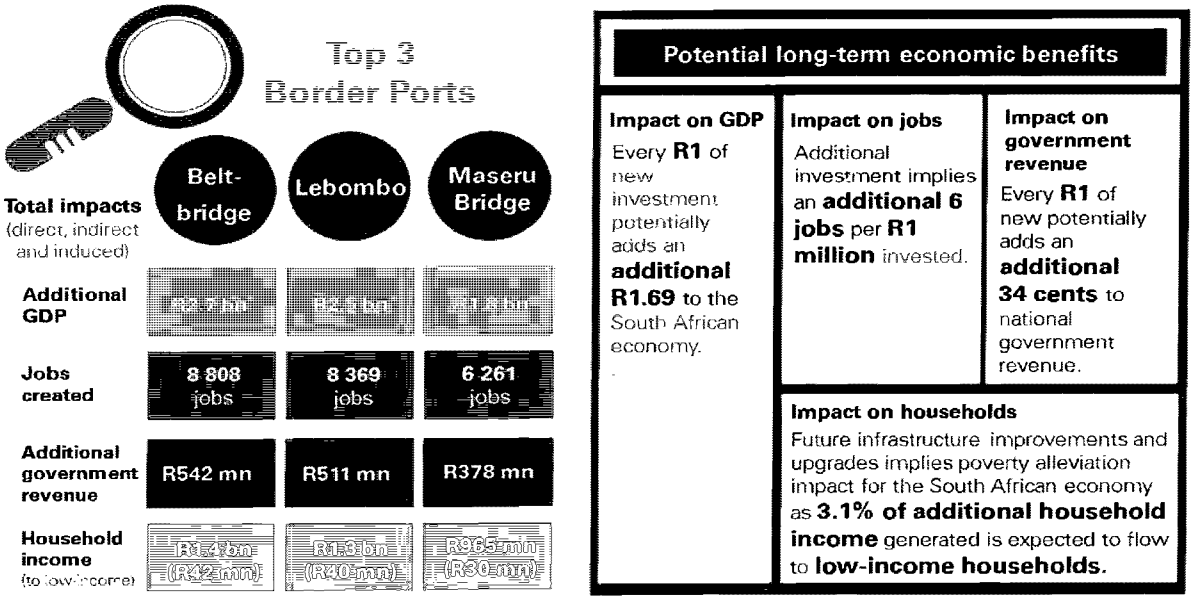
Figure 2.1: SADC transport corridors



2.2 OSBPs as strategic enablers of national and regional development

As indicated in the previous section, PoEs are key points along transport and trade corridors. The issue that needs to be considered is the importance of these corridors and land PoEs in attaining South Africa's policy goals and strategic objectives. Given a severely constrained fiscus, a strong case must be made for including the implementation of OSBPs in the programme to modernise South Africa's six largest land PoEs.

Figure 2.2: Economic contribution of the top three PoEs



Source: KPMG analysis from 2014 Social Accounting Matrix for South Africa

Africa contributes less than 3% to global trade; that contribution has not changed relative to the 387% growth[2] in international trade due to globalisation between 1980 and 2007. The growth of inter-African trade has also been minimal. There are two related reasons why Africa has not benefitted from globalisation and regional development. Firstly, patterns of industrialisation and trade scarcely changed when African countries gained their independence in the 1960s and 1970s. Africa still largely exports raw materials and imports finished products.

A major reason for the slow pace of Africa's industrialisation and the development of internal markets is its fragmentation into 54 States. Twenty-seven African countries have fewer than 10 million people, and 16 countries are landlocked without access to the coast. Without significant levels of cooperation and integrated planning and development, most will remain relatively isolated and underdeveloped.

In response to this situation, when economic growth began to accelerate in several African countries, African governments and institutions worked with international investors, who committed funds to develop trade and transport corridors. By 2012, investment in 10 transport and trade corridors in the sub-Saharan region reached $27,5 billion, committed over a period of 20 years.[3]

At an international level, integrated and modern approaches to border management have been promoted globally by the United Nations Economic Commission for Africa, the World Trade

[2] World trade, 1800-2015, Giovanni Federico, Antonio Tena-Junguito 07/02/2016, CEPR Policy Portal
[3] Trade Corridors: Key focus area for sub-Saharan African governments, Frost & Sullivan, 2012

Organization (WTO) and the International Organization for Migration, among others, supported by national agencies such as the Japan International Cooperation Agency. From an African perspective, a critical strategic goal is for intra-African trade to grow and build regional markets that drive integrated development and industrialisation.

At a conference in 2007, AU ministers responsible for border issues declared that there was a need "to put in place a new form of pragmatic border management aimed at promoting peace, security and stability, but also at facilitating the integration process and sustainable development in Africa." (Adopted by African ministers in charge of border issues held in Addis Ababa, 7 June 2007: paragraph 3)

This was later reflected in Aspiration 2 of Agenda 2063, which envisions Africa having "world-class integrative infrastructure that criss-crosses the continent" and "a continent of seamless borders, and management of cross-border resources through dialogue". The draft AU Border Governance Strategy was made public in 2017 but has yet to be formally adopted. The strategy has five pillars that are intended to guide the development of regional and national border governance strategies:

Pillar 1: Conflict prevention and border security

Pillar 2: Continental integration, free movement/migration and trade

Pillar 3: Cooperative border management

Pillar 4: Cross-border cooperation, borderland development and community involvement

Pillar 5: Border governance capacity development of actors and institutions.

On economic integration and trade facilitation, the draft AU Border Governance Strategy notes the potential for regional economic communities, free trade areas and the Programme for Infrastructure Development in Africa to have an impact on the four key sectors of transport, energy, trans-boundary water, and information and communications technology (ICT). However, the strategy goes on to stress, "Specifically, trans-boundary transport corridors can only deliver on their potential with cooperative border management and corresponding infrastructure, such as joint border facilities." [4]

At the Southern African Development Community (SADC) level, the summit of 2012 approved a Regional Infrastructure Development Master Plan. The introduction of OSBPs is one of the strategies that informed the plan. One of the first OSBPs was Chirundu, between Zimbabwe and Zambia. A 2011 evaluation found that the waiting time for commercial traffic was reduced from "about 4–5 days to a maximum of two days and often to a few hours".[5]

Table 2.1 below shows the relative size of South Africa's economy and trade, and **Table 2.2a** and **2.2b** show the direction of SADC exports and imports. It is notable that 45% of total trade

[4] African Union Border Governance Strategy, Final Draft of November 2017: p.25
[5] Data Collection Survey for Economic and Industrial Development along Economic Corridors in southern Africa: Final Report, JICA, May 2013, pp. 4–64

has shifted to the Asia-Pacific economic cooperation region, and only 3% of exports are from SADC to other African regions. The 13% of imports from Africa is largely oil and raw materials. However, as the SADC secretariat noted, "Total intra SADC imports have grown steadily over the past 10 years, more than tripling in total. As with intra SADC exports, imports also experienced a significant fall in 2009 due to the global recession." (SADC secretariat website, under facts and figures)

Table 2.1: Showing South Africa's contribution to key SADC economic indicators

Indicator	Information	Indicator		Data	South Africa
Member States	16, including South Africa	Trade	Total import	USD $185 243 million (2018)	USD $83 030 million 45% of total
			Total export	USD $191 575 million (2018)	USD $88 267 million 46% of total
GDP (2018)	USD $721,3 billion				Nominal, 2019 USD $371 billion 51% of total

(Adapted from SADC secretariat statistics, sourced from the IMF)

Table 2.2a: Overall direction of SADC exports (2000-2010)

Regional economic community/continent	Asian Pacific Economic Cooperation	European Union	Rest of world	Intra-SADC	Rest of Africa
% export	45	27	15	10	3

***Source**: IMF Direction of Trade, as reported by SADC secretariat*

Table 2.2b: Overall direction of SADC imports (2000-2010)

Regional economic community/continent	Asian Pacific Economic Cooperation	European Union	Rest of world	Rest of Africa
% import	45	27	15	13

***Source**: IMF Direction of Trade*

Tables 2.1, 2.2a and 2.2b above should be read with Figure 2.1 above showing SADC transport and trade corridors. In terms of patterns of transport, migration and trade, southern Africa

remains, to a large extent, locked into colonial trade and production relations. As the Reconstruction and Development Programme points out, this reinforces the outdated and essentially colonial structure of the South African economy, which is now geared to services and extractive industries with the industrial and agricultural sectors shrinking. South Africa has among the highest rates of unemployment, inequality and indebtedness in the world, which is racially skewed socially and spatially.

These factors impact not only South Africa, SADC's largest economy, but all SADC States, which held back by legacy colonial transport, trade and economic systems. They all face multiple challenges and risks such as unemployment, rising debt and political instability. There is also the growing impact of climate change on agriculture, energy, water[6] and food security. This, and related conflicts, cause mass migration with the constant threat of pandemics, terrorism and transnational crime.

There are positive global and African trends that present development opportunities. These require infrastructure and network development in energy, ICT and trade corridors. Improved governance and economic performance mean that some African countries are among the world's most rapidly developing economies. This has attracted investment and steps towards integrated development.

The west and east African regions, in particular the Economic Community of West African States and the East African Community (EAC), are making progress towards integrated development and infrastructure development. They are supported by regional and African institutions that effectively coordinate local and external funding and investment. These positive trends have created a policy climate that is conducive to the growth of Africa's industrial base, driven by intra-African trade and growth, and diversification of global exports.

A key factor in managing global risks and threats, and realising the vision and goals of Africa 2063, is developing regional and trans-regional networks of efficient, technology- and data-enabled corridors, with traffic facilitated through OSBPs. To enable this development to proceed, an enabling political, legislative and regulatory framework is required. The basis for developing such a framework was put in place in 2019 with the signing of the historic African Continental Free Trade Area agreement on 30 May 2019.

2.3 Enabler of national and regional security

PoEs and OSBPs are enablers for national and regional security. The concept of national security implies that a nation has self-determination, an internationally recognised territory and the capacity to secure its State and borders. The Constitution declares that South Africa is one, sovereign, democratic State. There can be no national security if the nation loses its sovereignty and its claim on the State. Under Chapter 11 of the Constitution, which deals with security services, the principles that govern national security are set out.

[6] Several states are dependent on hydro-electric power, now threatened by uncertain rainfall.

As indicated in the governing principles, national security must be pursued within the framework of the Constitution – internationally by promoting peace and security, and domestically by having a united nation that is "free from fear and want" as set out in Chapter 11, 198(a). National security is part of the core mandate of the security services, which encompass the SAPS, the SANDF and intelligence services.

While the security services' core mandate relates directly to national security, all organs of state have a national security responsibility and can request assistance from the national intelligence structures. The border environment is sensitive to risks and threats, and security is intelligence led. In view of this, all departments active in the broader border environment play active and important roles in national security.

All States use similar general principles when managing national security in the border environment.

Firstly, border management must always be risk-based, and:

(a) every effort must be made to deal with risks when they are outside the borders

(b) every gap in national security must be identified and dealt with as a potential risk

(c) it is important to separate low risks from high risks.

Secondly, border management should be efficient, secure, intelligence-driven and well-coordinated. Information must flow from all the departments based at a PoE concerning risks and threats, whether from abroad, within the border environment or domestically. Health Inspectors, for example, receive warnings of pandemics from the World Health Organization via the Department of Health. A plan to deal with a severe health threat will involve the security services, DHA, Department of Transport and missions abroad via the Department of International Relations and Cooperation. The SAPS, Sars and the DHA each play an important role in combatting transnational crime syndicates or terrorism at international, regional, national, provincial and border post levels.

PoEs are located at the point where countries interface with one another and, through that country, the rest of the world. They are also the point at which the border and corridor environments meet and regulate persons, goods and conveyances that cross that border. Officials at PoEs must be ready for any eventuality in a world characterised by globalisation and human and natural risks and threats to the sovereignty and wellbeing of nations and states.

2.4 Enabler of national and regional human rights

PoEs and OSBPs can also promote national, regional and global human rights. The relationship between sovereignty and human rights is often misunderstood. A nation and its citizens, individually and collectively, have a sovereign right to decide whether to apply capital punishment or allow refugees to live in their country, etc. One nation cannot, in general, legally compel another to expend resources on a category of persons unless very strongly established

agreements are in place, or they transgress or commit acts of aggression against another State or commit genocide. Matters are usually resolved at a political or diplomatic level, and usually in terms of individual cases and not through general agreements.

What the two countries can and must do, especially in the context of an institution such as an OSBP, is implement an agreement as a legal instrument for officials, mainly at an administrative level, to develop procedures and systems to resolve issues in ways that are efficient, effective, secure, reasonable, fair and humane.

An OSBP bilateral agreement must include provisions for the due care and protection of persons, and to uphold human rights commitments made by both states, as reflected in their respective laws and in international instruments they are signatories to, such as the UN conventions on refugees and trafficked persons.

In designing and establishing an OSBP, an audit of existing facilities, rules and procedures of both countries must be conducted by a joint technical working group (TWG). One objective of this audit must be to harmonise and simplify rules and procedures; a related objective must be to ensure that human rights standards are met.

Chapter 3: The OSBP policy context

3.1 Introduction

The high-volume commercial activity at certain land PoEs has become a major obstacle to national and regional economic development and security. Modernising key land PoEs is a strategic priority and an economic necessity. The increased cross-border movement of people, goods and conveyances between South Africa and her neighbours has led to congestion and lengthy delays at South Africa's PoEs. A re-think was necessary to speed up the clearance of goods, people and conveyances at PoEs.

The envisaged OSBP concept will be applied in the land PoE environment. The OSBP concept refers to the legal and institutional framework, facilities and associated procedures that enable goods, people and vehicles to stop at a single facility to undergo the necessary checks and controls, following applicable regional and national laws, to exit one State and enter the adjoining State. This is contrary to a traditional two-stop border post concept in which exit procedures are carried out on one side of the border and entry procedures are carried out on the other side for persons, vehicles and goods. Except for the Lebombo PoE, all of the land PoEs in South Africa are based on a two-stop border post model.

The ideal solution is to establish OSBPs where vehicles, goods and people stop only once for border processing formalities. Through a negotiated bilateral agreement, officials from both countries will operate in a common control zone (CCZ), where they will apply procedures that are secure, simplified and harmonised. Through cooperation on implementing the OSBP solution, both countries enhance their capacity to manage the PoE and enforce their laws. These improvements contribute to growing the economy by strengthening key drivers, including trade, tourism and investment.

Strategically, OSBPs could in future contribute to improved regional integration by enabling goods and people to move swiftly within SADC and the continent as a whole. The continental north-south corridor also stands to benefit directly from OSBPs being established between South Africa and its neighbouring countries.

3.2 Problem statement

Poor transport infrastructure is a colonial legacy that is often cited as a major reason for low levels of industrial development and the underdevelopment of African markets. Investment in roads and railways is essential, but the benefits are limited if PoEs on major corridors remain places where people queue for hours and it takes days to clear a truck carrying goods. The main problem is that moving people, freight and conveyances at PoEs is ineffective and inefficient, and has a negative impact on all categories of legitimate travellers and users of the port, from major exporters to a tourist or a local trader who conveys goods on a bicycle. Much of this is due to the following factors, which are present to varying degrees at all PoEs:

(a) Goods, vehicles and people must stop multiple times to be cleared on both sides of the PoE.

(b) Legislation, rules, processes and procedures used by the respective countries are over-complex and incompatible with facilitating the movement of goods, conveyances and people.

(c) Technology and data use is limited within the PoE and at a systems level, which limits the ability to complete online preclearance procedures before goods, vehicles and people arrive at a PoE.

(d) Infrastructure and equipment at PoEs are outdated, and PoEs are designed for economies based on migrant workers, the export of raw materials and a minority of privileged travellers.

(e) Data sharing and coordination between countries, between their respective government departments and within departments is lacking.

(f) Accurate, real-time data that could enable efficiency, security and effective management across the whole logistics value chain is lacking.

(g) Weak controls, security and enforcement result in unacceptable levels of crime and corruption and create risks and threats for travellers, staff and national security.

(h) Management systems and structures at PoEs are fragmented and there is no integrated border management with a lead agency.

(i) Basic human rights requirements and standards are not adhered to, such as adequately providing basic facilities and support services for travellers and staff at PoEs.

(j) Non-tariff barriers in the form of unnecessary controls, charges and restrictions are imposed by one or both governments.

Designated PoEs are an integral part of managing the border environment to minimise risks and threats and maximise opportunities and benefits. The problems listed above indicate that South Africa has not invested in sufficient capacity to achieve this. The capacity to coordinate across all spheres of government and relevant agencies is essential; creating the BMA will greatly assist in this regard. For example, for a conveyance to transport radioactive material across a border safely, agencies of the departments of Energy, Trade and Industry, Transport, Police and Agriculture, Forestry and Fisheries must liaise with those responsible for the PoE. An accident or an attack could result in catastrophic contamination of the environment or a national key point such as the border post or a power station. Currently, the necessary level of coordination and security cannot be assured.

3.3 The OSBP framework

Ideally, as a pre-requisite for being functional and sustainable, OSBPs should be rooted in a sound policy and underpinned by an enabling legal framework and implementation strategy. The process of developing an OSBP policy in South Africa commenced in 2014, under the

auspices of the National Treasury, with a policy discussion paper (OSBP framework) to establish OSBPs. In 2015, this project was handed over to the DHA, as the designated organ of state, to coordinate border management activities in South Africa, including the responsibility for establishing the BMA. In December 2018, Cabinet approved the OSBP framework requiring South Africa to adopt an OSBP policy and subsequent legislation. The OSBP framework provides guidance and guidelines, and is the first step towards developing a more coherent policy and regulatory regime to establish OSBPs in South Africa. It is intended to enable lessons to be learnt for the future development of a more comprehensive national OSBP policy and legislation.

The following principles will guide the establishment of an OSBP:

(a) Before pursuing an agreement, a business case for a particular proposed OSBP must be made to, in part, establish the economic viability of the proposed OSBP, largely through an assessment of the estimated costs and benefits of a proposed OSBP.

(b) Strong political drivers at the highest levels from both countries should be in place before an OSBP is implemented. This will include a memorandum of understanding between the two relevant countries supported by a legal framework allowing extraterritorial authority to implement an OSBP system.

(c) The OSBP policy and legislation must be implemented in compliance with South Africa's regional and multilateral commitments in trade facilitation, immigration, transport corridor management, security and other related commitments.

(d) The OSBP policy and legislation must also be implemented in compliance with South Africa's related national policies, including policies and strategies on integrated multimodal transport planning, freight logistics, trade and transport corridors and national road, maritime and rail transport plans and strategies.

(e) Cost sharing between South Africa and the affected neighbouring country shall be an important principle in establishing an OSBP. The rationale for cost sharing is that the intended benefits of OSBPs are meant to be of mutual value to the affected parties. Therefore, the costs and resources required must be equitably shared between South Africa and the affected neighbouring country.

(f) Cost sharing shall also explore various financing options, such as public financing, internally-generated revenue, development assistance, borrowing from multilateral financing institutions, borrowing from the private sector, and public-private partnerships.

(g) All financial and other resource implications of an OSBP must be specified and quantified before its establishment. The manner in which South Africa and the relevant neighbouring country will provide for financial and other resources required will be clearly spelt out in a formal agreement between the two countries.

(h) The OSBP must be designed in the most economical and cost effective way possible. The design process will be guided by detailed studies to be conducted on both sides of the border to assess what is already in place in terms of infrastructure and procedures.

(i) OSBPs must be designed as environmentally-friendly and customer friendly as possible, especially considering the needs of small-scale traders.

(j) The OSBP design must ensure that security, safety and revenue collection are not compromised.

(k) OSBPs will apply intervention by exception. Unless there is a reason to challenge a driver, importer or traveller, traffic should be subject to minimal controls. The design of the OSBP will facilitate trade and move low-risk traffic rapidly, with a secondary search/control ability for all agencies.

(l) When a vehicle is targeted for a more detailed check, this will take place off lane, so that upstream traffic is not delayed. The standard will be that any intervention expected to last more than one or two minutes should lead to the vehicle being diverted to a secondary inspection bay within the CCZ.

(m) The process of introducing an OSBP will be accompanied by a change management process.

(n) Internal consultative meetings at a national level will be convened prior to convening stakeholder meetings involving both countries.

(o) The bodies or agencies of both countries responsible for implementing the OSBP will sign off on the standard operating procedures before designing the physical infrastructure and subsequent implementation commences.

(p) Both private sector and public sector stakeholders will be consulted on the design and implementation of the OSBP.

(q) Subcommittees dealing with ICT, facilities, processes and procedures, and legal issues will be set up for the proposed establishment of each OSBP before the design work commences, and will continue to meet as long as it is considered necessary to do so.

(r) The relevant bodies or authorities will ensure that adequate ICT and telephonic structures and systems are in place to allow for effective and efficient service delivery at the PoE.

Over and above the OSBP policy and subsequent legislation, OSBPs will be governed by bilateral agreements between South Africa and each neighbouring country willing and able to share OSBPs with South Africa. Such legal instruments will enable the border agencies of each State to apply their national laws in a territory of the adjoining State. As national laws cannot automatically be applied in other territories, specific provisions will be developed to give such agencies extraterritorial jurisdiction.

3.4 The Lebombo OSBP pilot

In September 2007, South Africa and Mozambique signed an OSBP agreement to implement OSBP solutions at specified PoEs along their border. The OSBP agreement was ratified by the

legislatures of both countries. Steps taken by the bi-national working groups established to implement the OSBP agreement included feasibility studies, determination of processes and procedures, and an analysis of relevant legislation with a view to identifying required changes. The OSBP agreement was ratified by the legislatures of both countries. The Lebombo-Ressano Garcia PoE was selected for conversion to an OSBP, with a straddled model adopted given the physical proximity of the existing ports.

A key element of the OSBP agreement is to provide for extraterritorial jurisdiction at commonly held border posts and to deal with processes and procedures for arresting and detaining people and seizing goods. The OSBP agreement also entitles both parties to apply their own domestic laws applicable in the border environment within the CCZ and includes provisions aimed at facilitating rail traffic across borders.

Funds were secured to begin construction and interim measures were put in place to improve the efficiency and effectiveness of facilitating commercial traffic. Of most significance was the establishment of satellite facilities on the approach roads to the PoE, four kilometres from Lebombo and seven kilometres from Ressano Garcia, where officials from both countries provided preclearance for vehicles and freight. This arrangement was based on the partial implementation of a juxtaposed model of an OSBP, while the drivers of private vehicles and travellers on foot were processed separately, but in the same complex, by officials of the respective countries working on each side of the borderline.

Currently, the OSBP solution is only partially implemented for both commercial and private traffic, with elements of both a straddled and a juxtaposed model adopted to improve efficiency. CCZs have not been established and the new infrastructure and facilities are only partially built. Levels of service, security, compliance and enforcement fall short of the standards required for a fully functioning OSBP. Harmonisation of processes, legislation, systems and information sharing is limited. However, through improved cooperation between the states, some processes have been improved and efficiencies have been realised. This is mainly in terms of commercial traffic and arrangements made to deal with heavy volumes during the festive season.

The failure to complete the project can mainly be attributed to weak governance and a lack of sustained commitment, a limited understanding of the full concept of an OSBP (regarded as mainly an infrastructure project) and finalising investigations related to the infrastructure development. The absence of a national OSBP policy framework and subsequent legislation also contributed to the failure. Going forward, a new project will have to be initiated, with the intention of building on what has already been achieved and lessons learnt through experience gained elsewhere in establishing OSBPs.

SECTION B: OSBP POLICY STRATEGIC INTENT

Chapter 4: Policy thrust and vision

4.1 Introduction

Drafting a new policy must be justified by defining the problem, how it will be addressed and a vision of what will be achieved if the policy is implemented. Studies on the implementation of OSBPs in Africa, Asia and the Americas show that a frequent cause of failure is the lack of a shared vision of the purpose and nature of the project. This chapter sets out the policy framework and strategic intent of the OSBP project to steer all stakeholders towards a common goal.

4.2 Vision statement

OSBPs that facilitate seamless, safe and efficient passage for people, conveyances and goods across South African land PoEs without compromising the sovereignty, development, national security or international obligations of South Africa.

4.3 Intended outcomes of the OSBP policy

The OSBP policy seeks to achieve the following outcomes:

a) Increased economic integration with neighbouring countries across SADC and the continent

b) Faster, more efficient and economical facilitation of movement for legitimate goods, conveyances and persons through land PoEs

c) Better enabling conditions to facilitate trade, including economic growth and job creation

d) A flexible corridor system that is strategically managed using digital technology

e) Enhanced collective responsibility for national and regional security, including managing threats to territorial integrity, biosecurity, public health and the environment

f) Honour human rights and humanitarian obligations in line with the Constitution and international agreements.

4.4 Key foundational principles of OSBP policy

4.4.1 National interest

Establishing the OSBPs with neighbouring countries will enable South Africa to extend its borders. That is, the OSBP will enable South Africa to apply its border management controls extraterritorially while granting the same privilege to an adjoining State. However, such an arrangement will primarily be informed by South Africa's national interest, which should be defined in accordance with the following:

- The supremacy of the Constitution, including principles underpinning the Constitution
- National priorities such as national security and development
- Promotion of human rights, peace and stability in order for South Africans to live in a secure, stable and prosperous world
- Respect of, and adherence to, the rule of law.

4.4.2 Extraterritorial jurisdiction

It is an established legal principle of public international law that national laws of a State generally only apply within the territory of that State: "The exercise of jurisdiction is limited, save by special international agreement, to the territory of each State, so that the State can only exercise it over persons or things within or coming within the territory."[7] In what amounts to a paradigm shift, the principle of extraterritoriality or extraterritorial jurisdiction allows a State to extend the application of specific national laws to a place physically located outside its own territory.

Given that the establishment of an OSBP does neither moves the physical international border or territory, nor cede it to an adjoining State, legislation must be enacted to stipulate applicable and non-applicable jurisdictions in the OSBP geographical area. That is, the OSBP enabling legislation in both countries must enable border officers of the respective countries to carry out their applicable national laws in a CCZ in the adjoining State and provide for hosting these officers. The bilateral agreement must clearly stipulate national jurisdictions and/or duties, powers and functions that will not be applicable in an OSBP or CCZ.

4.4.3 Reciprocity

In international law, reciprocity describes an environment in which states agree to cooperate on a matter of **mutual interest** by balancing rights and responsibility towards one another. An

[7] J.E.S. Fawcett, The Law of Nations, 1968, p. 54; quoted in the JICA OSBP Sourcebook, p. 8-13

OSBP that is efficient and secure is of mutual interest to participating states, and the bilateral agreement must clearly stipulate areas of cooperation and associated responsibilities towards each State. Areas of cooperation would include hosting arrangements, and a reciprocal application of border control and enforcement laws, systems and procedures in the territory where the CCZ is located.

4.4.4 Harmonising procedures

Establishing OSBPs requires harmonised border crossing procedures for people, goods and conveyances. Designing buildings and facilities, ICT systems and traffic segmentation without consensus on new processes and procedures will result in ineffective OSBPs. The OSBP bilateral agreement or manual should clearly stipulate the new processes and procedures that will be harmonised to allow for border controls to be processed expeditiously. This will include harmonisation of procedures in the following areas:

- alignment of opening hours for OSBP partner States
- information sharing by countries
- sharing facilities, equipment and other resources by border agencies (e.g. scanner, weighbridges, sniffer dogs, etc.)
- traffic segmentation
- sterility of the OSBP
- payment of levies for the use of the OSBPs
- jurisdiction in case of offences
- preclearance
- privileges and immunities of foreign officers.

4.5 Key defining features of the OSBP

A land PoE must satisfy the following criteria to be legally classified as an OSBP:

(a) It must be a single land PoE, established and recognised by two or more countries that share a border, to enable the more efficient, effective and secure facilitation of the movement of persons, goods and conveyances across the border.

(b) It must be legally based on, and governed by, a bilateral or multilateral agreement that has been concluded in accordance with the domestic laws of both countries.

(c) Policies, legislation, systems and procedures relating to the main functions of a PoE must have been simplified and harmonised by both countries to enable a person, conveyance and goods to be cleared at a single point.

(d) Implement one-stop border processing arrangements in each country by establishing and designating control zones (common and exclusive) at their respective common border posts. The control zones may, with the agreement of the two states, be juxtaposed, straddled, wholly located in the territory of one State or follow some other mutually agreed configuration.

(e) The control zone must enable border officials of the respective countries to apply their respective border law enforcement legislation within the agreed control zone.

(f) Extraterritorial jurisdiction for each country must be clearly articulated in the bilateral agreement.

4.6 Implementing the OSBP approach

The following minimum elements of the OSBP must be jointly implemented by the two countries:

a) Legislation, systems and procedures relating to the main functions of a PoE must be simplified and harmonised by both countries to enable people, goods and conveyances to be cleared at a single point.

b) Control zones must be established in one or both countries where officials can apply their respective identified border laws (or specific provisions) as defined in enabling legislation in their countries.

c) The respective identified border laws and related provisions must address and enable all the relevant border law enforcement functions, powers and duties that need to be executed within the OSBP control zones.

d) Digital data or information must be exchanged where necessary in the context of simplified processes and procedures.

e) Bilateral and domestic governance, administrative and financial arrangements must be in place to enable the sustained operation of an OSBP.

f) Stakeholders must be consulted, and kept informed or involved as appropriate in developing OSBP policy and the OSBPs themselves, in line with constitutional principles and good governance.

Chapter 5: Different models of OSBP and South Africa's preferred model

5.1 Introduction

A traditional two-stop border post is completely separated by the border line, although there may be various forms of cooperation in place. Each country maintains separate facilities, systems, processes and procedures and exit and entry roads. Travellers, goods and vehicles go through at least two sets of procedures, located at the two respective border posts.

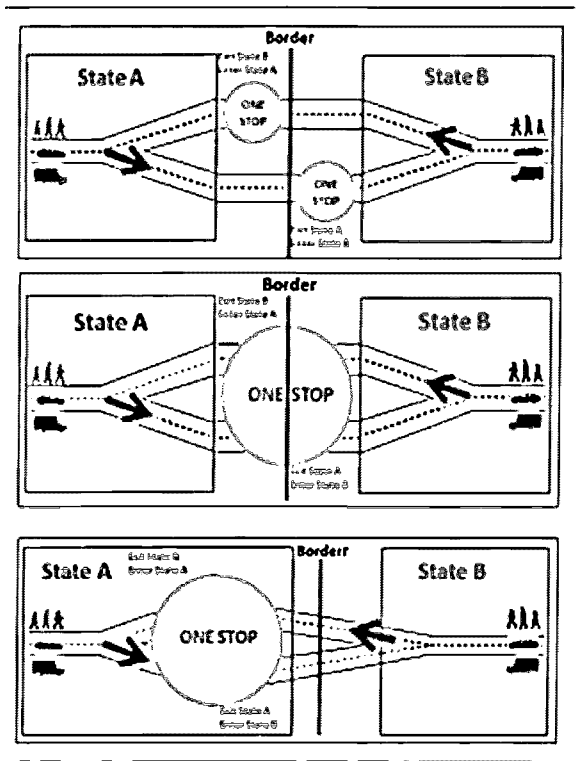
There are three generic ways in which two countries can cooperate in operating an OSBP that facilitates the cross-border movement of people, goods and conveyances in an efficient and effective manner. These three options - the three OSBP models - are compared in Figure 5.1 below.

Figure 5.1: The three OSBP models compared

Juxtaposed OSBP: Officials of both countries are based in a common extraterritorial control zone in the "country of entry". Officials of the country being departed clear for exit, whilst their colleagues from the country to be entered clear for entry. Their respective systems are harmonised, and data is exchanged.

Straddled OSBP: The border post is built on the border line with a common control zone where people stop once to be cleared by officials of both countries. Systems are harmonised and data is exchanged.

Single Country OSBP: One country relocates its entire clearing process to a common extraterritorial control zone in the other country. Systems are harmonised and data is exchanged.



The three generic OSBP models have the following basic characteristics in common.

(a) There is one PoE and both countries are responsible for

(i) the part that falls within their territory

(ii) shared facilities according to an agreement.

(b) The three models employ the same OSBP methodology.

(c) There is no change made to the international border line.

(d) Some officials from both countries operate in a designated CCZ, the location of which varies according to the model being implemented, as shown in Figure 5.1 above.

(e) Legislation must be in place to allow officials to apply the specified laws of their country extraterritorially in the CCZ. This does not extend to matters that must be referred to the respective states' criminal justice systems.

5.2 Definitive features of each of the OSBP models

The juxtaposed model

The two countries sign an agreement that establishes a CCZ in each of their territories where relevant officials of both countries can apply specific laws. The main advantage is that there may be fewer issues relating to sovereignty, as neither country must give up a physical border post and existing facilities can be adapted to suit the prevailing circumstances. A related advantage is that the model is reciprocal in nature, with each country having similar roles, expectations and responsibilities. There are fewer legislative changes compared to the single-country models, as the hosted officials will have a comparatively restricted set of functions. Risks can be managed more effectively as the flow of traffic is designed in such a manner that officials of State A based in State B process people, conveyances and goods exiting their country, while officials based in their own territory clear traffic that is entering their country.

One disadvantage is that for the port to function efficiently and effectively, both states must meet their obligations fully in hosting the officials of the other State. This requires sustaining high levels of commitment and cooperation. It also requires robust governance structures and arrangements to be in place to ensure, among other matters, that conflicts can be resolved. The model is flexible, and the PoE can continue to function if the basic agreement is adhered to, without implementing or sustaining some key elements of OSBP methodology. However, this is also a disadvantage as the benefits of the OSBP methodology will not be realised if preclearance is not done by both states, systems are not harmonised and data is not exchanged.

The straddled model

Geography and existing infrastructure may create conditions for the CCZ to be established on the border line. The main advantage is that issues of sovereignty, legislation and extraterritorial jurisdiction may be simpler and easier to deal with. A CCZ will straddle the border line, with the same extraterritorial jurisdiction granted in the other two models being legally granted to designated officers. However, the range of laws they administer may be more limited and there may be fewer disputes and complications arising from cases that must be referred to the criminal justice systems of the respective countries. The main reason is that, in general,

criminal justice systems do not enjoy extraterritorial application and, in the straddled model, states have clear jurisdiction up to the border line.

This positive factor could potentially reduce the time required for negotiations and the substantial time required to create a viable legal basis for the PoE to operate. South Africa and Mozambique have a ratified OSBP agreement that applies to any OSBP that the two countries might establish, which was negotiated over a relatively short period with the intention of establishing a straddled OSBP at Lebombo. One reason for the relatively short period of negotiation was that there appeared to be few changes needed to existing legislation.

Disadvantages may include challenges in adapting existing port infrastructure and facilities. Straddled PoEs are possibly less costly to establish on greenfield sites where a purpose-built structure can be put in place that straddles the borderline. There must be enough space for segregation of traffic (such as commercial and private conveyances) in terms of approach roads and flows within the PoE, and for additional zones and facilities.

In a juxtaposed model, the traffic flow can be designed for officials operating on the territory of the other country to clear traffic entering their country, while officials of the host country clears those exiting their country. In a straddled model this division of labour, which helps to manage risks, may be harder to achieve or require more expensive technology and infrastructure. This reduces the funds available in critical areas such as simplifying, automating and harmonising processes, procedures and systems.

The single-country model

In this model, one country relocates its entire PoE one-stop operation to the territory of the other. The reason might relate to local geography or the host country might have more resources. As a holistic solution, this model has few advantages and the juxtaposed or straddled model is almost always to be preferred.

The main disadvantages relate to issues of legislation, extraterritorial jurisdiction and sovereignty. Both the host country and the hosted country will have to make extensive changes to their domestic legislation to enable the wide range of functions at a PoE to be performed in an extraterritorial control zone. Complex arrangements will have to be agreed on referring cases to the criminal justice systems of the respective states, returning persons, goods and conveyances, and officials operating and possibly staying in the host country.

Such asymmetrical circumstances require stable relationships between countries and a high level of trust. Disputes may arise between the two countries regarding sharing the costs necessary to run operations and purchase and/or maintain facilities. These risks will be particularly pronounced if there is a wide gap in the level of development between the two states.

5.3 Factors to consider when selecting a model of OSPB

The choice of a preferred model is dependent on bilateral diplomatic relations, existing facilities, geographical constraints and a cost-benefit analysis given the building of new infrastructure and the value derived from traffic passing through the PoE. It also involves finding a common vision for the future development of the PoE over a 15 – 20-year period, as well as the transport corridor passing through it.

Just as important is assessing the kind of relationship that could be developed between the countries and the risks involved. For an OSBP to function efficiently, effectively and sustainably, a minimum level of good governance and trust is needed to ensure the necessary level of cooperation. Other important factors are the funding model adopted by each country, and their willingness to establish a viable legal framework, to simplify and harmonise rules and procedures and to enforce border laws and regulations.

Given these considerations, each OSBP project will have unique features. A comprehensive and creative solution must be negotiated and set out in a bilateral agreement. The degree to which the regional context makes this process possible is important. South Africa is a member of SADC, which unlike the EAC, does not have a common OSBP policy or legislation in place, and is less advanced in terms of the integrated planning of trade and transport corridors. One of the factors that enabled integrated regional development in the EAC is that the six countries of the EAC have comparable economies and levels of technical development. The South African economy is far larger and more complex than those of the other 15 SADC member states.

5.4 The possibility of mixed OSBP models

A coherent OSBP solution for a PoE would involve selecting one of the three models as a basis for governance and legislation. However, elements of the other models could be incorporated, even if only for certain phases of the development. This approach provides the flexibility needed to implement OSBP projects in complex and dynamic environments. For example, it may be necessary to locate an OSBP function, such as application of sanitary and phytosanitary measures, in one country if the necessary facilities were only available in that country.

Another example is to have joint teams, as prescribed in the juxtaposed model, operating in zones located away from the main PoE, which may be based on the straddled model. This is the case at Lebombo where commercial conveyances are precleared by joint teams at sub-posts established several kilometres from the intended straddled OSBP port on both sides of the border. This arrangement continued even after the failure of the larger project, although without the benefits of it being part of a larger OSBP solution. It could be retained for a period after re-establishing the project, though it would benefit from having a stronger policy and legal basis. It could be discontinued once online preclearance and the development of the OSBP was sufficiently advanced.

The use of increasingly integrated technology to automate and manage processes and generate data will allow complex solutions to be implemented that would further allow flexible approaches to the use of OSBP models. For instance, central biometric access could be used to measure the use of equipment accessed by officials of the respective countries and per-second billing would be enabled by smart accounting and management information software. Carrying out these functions manually would cause delay, be vulnerable to abuse and corruption and likely result in disputes.

5.5 Options and recommendations

A country could have objective reasons why it declares its preference for a specific OSBP model. Declaring a preference would help a country to plan and to budget for legislative, systems, human resources and infrastructure requirements.

Policy options:

The OSBP policy should either:

a) state a preference for an OSBP model without qualifications

b) not state a preference for an OSBP model

c) state a preference for an OSBP model with qualifications.

Policy recommendation:

Option (c) of the policy options above is recommended as the preferred option, with the preference being for the **juxtaposed model**. The motivation for this recommendation is as follows:

- It is likely to make the best use of existing facilities
- Usually, it creates fewer problems related to sovereignty and is symmetrical in terms of obligations placed on both states
- It is the most flexible and can incorporate elements of the other two models
- Given the levels of asymmetry in development between South Africa and its immediate neighbours, the juxtaposed model enables South Africa to better manage socio-economic and border-related risks
- The juxtaposed model works better with the existing geographic and topographic conditions
- The juxtaposed model provides financial benefits in relation to incinerating unwanted agricultural products

- The juxtaposed model is flexible and could allow for reverting to the traditional PoE model should there be a change on the grounds of posing a security risk to the country
- The juxtaposed model is generally preferred in Africa and by most of South Africa's neighbouring countries, with more lessons that can be learnt.

While stating a preference for a juxtaposed model, South Africa will keep other options open. Geo-political or funding factors, for example, may lead to another model being chosen or aspects of other models being incorporated into the design of the OSBP. Therefore, the preference for a juxtaposed model is informed by historical and current factors that are not fixed. Should the factors change in future, South Africa will consider implementing other models.

SECTION C: OSBP OPERATING AND LEGISLATIVE MODEL

Chapter 6: OSBP operating model

6.1 Introduction

The main purpose of an OSBP is to enable rapid and secure facilitation of the movement of people, conveyances and goods across the land borders. To achieve this goal, both countries must implement the following five key OSBP pillars:

- Put in place a policy, legislative and governance framework
- Establish an OSBP extraterritorial jurisdiction
- Simplify and harmonise processes and procedures
- Establish and manage the ICT and data exchange capacity
- Establish and manage hard infrastructure and facilities.

6.2 Extraterritorial jurisdiction of the OSBPS

Without extraterritorial jurisdiction there cannot be a CCZ where officials of both countries apply their respective legislation, and this arrangement is at the centre of OSBP approach. Unless there is domestic agreement among all the relevant internal stakeholders on how to approach extraterritoriality at a policy level, the project should not proceed.

Foreign missions in a country are protected by international laws and by bilateral agreements that give them the right, to a defined extent, to apply their own law in defined zones in the territory of another country. Two areas require the host country to put legal instruments in place. One is the exemption of designated foreign officials from the jurisdiction of a host country. The other relates to hosting arrangements, which include the functions foreign officials are authorised to perform. In making these provisions the borders of South Africa, its Constitution and its criminal justice system remain essentially unchanged.

The same broad principles apply in the case of OSBP common control or exclusive control zones, and arrangements made for areas outside the zones such as joint training and operation or emergency procedures. There are no changes to borders; the control zones and limited rights accorded to another State exist because of agreements that can be changed or rescinded. Governance and control depend on establishing and managing applicable legislation, institutions, rules and norms. Internationally, the enabling legal instrument created is an OSBP Act that, among other things, creates the legal basis to establish common and exclusive control zones.

Providing officials of another country access to government zones, officials, operations, data, information and systems – and giving them the right to extraterritorially apply their laws – creates risks and opportunities for both countries. To mitigate the risks, all the elements listed above must be strictly limited, clearly defined and ratified through a bilateral agreement that, *inter alia*, has provisions covering jurisdictions, conduct, disputes and emergencies. The opportunities will be to raise the level of cooperation and the efficiency and security of both states, and to achieve large savings in time and costs.

6.2.1 Delimitation of the physical location of the OSBP premises

The control zone is at the heart of all OSBP models. Essentially, the designated laws, systems and border controls of two countries are applied in a common space that can either be in one of the countries, be replicated on both sides of the border or straddle a border. The models vary according to how expensive, difficult or risky they are to implement and operate. However, the policies, laws and systems of the respective countries, and the agreement they sign, should largely determine how the officials work within a control zone regardless of a model.

International practice demonstrates that the configuration of each OSBP's control zone is agreed between the two partner States that have a common OSBP. The control zones shall be arranged so that, for each direction of travel, border controls will be carried out in the State of entry and, depending on the configuration, from a single stop location. The physical location and spatial extent of the OSBP premises will need to be defined in the bilateral agreement. That means a control zone will comprise the specifically demarcated and secured physical areas that are mutually agreed between the relevant partner States. This delimitation should include the definition of the CCZs within which officers from both states will perform controls and in which they may circulate freely. It should also define the areas set aside for the exclusive use of each State's officers.

6.2.1.1 Common control zone (CCZ)

The CCZ means the geographical area designated and delineated within, or as part of, an OSBP for the purposes of jointly executing border law enforcement controls. The following border controls, *inter alia,* will be exercised by officials of both countries within a CCZ:

- Immigration controls
- Customs and revenue controls
- Port health/biosecurity controls
- Environmental management controls
- Agricultural/phytosanitary controls

- Border policing
- Cross-border roads, traffic and transport controls
- Safety and security controls
- Border infrastructure development and maintenance.

6.2.1.2 Exclusive use zone

Exclusive zone refers to facility or an area designated within the CCZ of the host partner State for the respective exclusive use and access by border officials of the adjoining partner States for the execution of border controls and related matters. This means that South Africa will grant border officials from the adjoining State access to a working area set aside for their exclusive use; and a similar provision will be made for SA officials in the adjoining State.

The international practice[8] shows that, in order to protect each State's interests, the host State agencies may not enter an exclusive area, except at the express invitation of an officer from the neighbouring State. The only exception to this principle is where a law and order offence has been committed in an exclusive area and the police officers of the host State may enter that area without permission, provided they would otherwise have the power to enter premises under their own law. Such powers may only be exercised for the purposes of making arrests (if applicable) or otherwise obtaining evidence. However, it is strongly recommended that these powers be exercised based on clear joint operational procedures agreed to by the partner States.

6.3 Extraterritorial application of laws in the CCZ

A distinction is usually made between offences committed in terms of border law enforcement legislation (e.g. immigration) and those committed in terms of criminal law legislation (e.g. murder, theft). In the former case, each State has jurisdiction over offences under its border law enforcement legislation that are detected while its officers are undertaking their controls. In essence, officers enforcing the border laws and procedures in a control zone must do so according to the border law enforcement legislation of the State that they work for. Once the State's officers have completed their border controls, they no longer have jurisdiction on border law enforcement matters, except with the agreement of the officers of the other State.

Regarding criminal law offences, the accepted approach is that jurisdiction lies with the country in whose territory the offence has been committed. Criminal offences will be dealt with according to the territorial jurisdiction of each State and may not be confined to the OSBP arrangements. In other words, a crime that is committed in the adjoining State, whether or not border control procedures have been concluded, shall be considered as a crime that was

[8] JICA OSBP Sourcebook (2016): pg. 8-15

committed against that State. Law enforcement authorities of both states will enter into an agreement for enforcing such provisions.

6.3.1 Extraterritorial application of border law enforcement laws

International practice shows that where the CCZ is in the adjoining State, border management officers (immigration, customs, health, etc.) of the exit State retain jurisdiction until all border controls have been handed over to the officers of the adjoining country. South Africa will adopt a similar principle with regard to the application of border law enforcement. That is, where the CCZ is in Mozambique, South African border control officers retain jurisdiction between the borderline and the CCZ (as long as all border controls have not been handed over to the Mozambican border officers).

As a matter of principle, in the CCZ in the adjoining State, a South African officer has the same powers as they would have working within South Africa under the border control laws, subject to any exceptions defined in the enabling legal instruments. The powers of an officer working in the adjoining or host State are only restricted by the action of handing over control. Once a control has been handed over to an officer of the receiving country, the officer of the exit country can no longer exercise that power, except with the express permission of the officer of the State to whom control has been handed. Exit formalities should therefore be completed before entry formalities may start. Jurisdiction moves from the country of exit to the country of entry once exit formalities have been completed.

6.3.2 Extraterritorial application of criminal laws

It is an established principle in international law that a crime can only be prosecuted and tried in the territory where it took place. For such a jurisdiction to be extended to another State, international or regional measures including agreements, and institutions like courts and parliaments (legislative jurisdiction) must be established. This is the case in the EAC region where a regional legislation, court and Parliament are in place to deal with the extraterritorial criminal jurisdiction. Given the absence of such regional measures in SADC, the bilateral OSBP agreement must specify how such cases will be prosecuted and tried, including escalation and conflict resolution procedures.

International practice in the extraterritorial application of criminal laws within the OSBP arrangement shows that general law enforcement powers are within the competence (authority) of the host country police. Therefore, a police officer's general law enforcement powers (e.g. under the Criminal Procedures Act) is restricted to each State's national territory. This implies that each police agency has general law enforcement jurisdiction within its national territory, and police officers cannot exercise general law enforcement powers extraterritorially. If a criminal offence (e.g. murder, theft, assault) is committed in the CCZ of the country of entry, even if the immigration control has not been handed over by officials of the exit country, police officers of the country of entry will have jurisdiction.

6.3.3 Officials' immunity from the criminal jurisdiction

Officers from the exit State enjoy immunity from prosecution by the host State for any action related to the performance of their border control functions. Such offences are dealt with by the officers of the State that will have jurisdiction in terms of its laws. However, such officers' immunity does not extend to criminal offences. If an officer from the exit State commits a criminal offence in the host State, he or she is subject to the criminal jurisdiction of that host State.

6.3.4 Safety and security management of the CCZ

The host partner State is responsible for ensuring the safety and security of the CCZ, officials and assets of both the adjoining partner State and the users of the border control zones that access the OSBP for services. However, for national security reasons the adjoining partner State will be allowed to enhance such security measures for its officials and assets in the host State's CCZ. Such measures will be undertaken in compliance with the applicable laws of the host country.

Law enforcement officers of a host State with responsibility for maintaining peace, security, and law and order in the CCZ may carry such arms as are mandated in their national laws to discharge their obligations. The type of arms carried should reflect the perceived security threat within and around the OSBP and the sensitivities of the travelling public to carrying such arms.

The adjoining State's law enforcement officers may not carry arms in the host State's CCZ, regardless of whether carrying such arms is mandated by their national laws, except by special arrangements with the host State. Such special arrangements may include carrying arms or non-lethal safety and security equipment by officers through the CCZ to the adjoining State's exclusive use areas, where it has full control and security responsibilities. Similarly, the type of arms carried in such exclusive use areas shall be with due regard to the security threat to such areas and the sensitivities of the travelling public that may have access to these areas.

6.4 Human resource considerations

With respect to matters relating to human resources, the Constitution and labour laws oblige the State as an employer to make provision for any substantive changes to the conditions of service of officials working in another country. Some standards that have to be met may require additional training, such as acquiring language skills. Respective domestic consultations with organised labour formations would have to take place as prescribed in existing legislation.

Officials of the adjoining State who are appointed to perform OSBP-sanctioned functions in the control zone of the host State:

a) shall be provided with State tools of trade as required by their job functions

b) may receive a State guarantee against any personal damage or loss, which are only covered by their insurance policies when they happen in the adjoining and not host State

c) shall suffer no deprivation of the conditions of employment. The Labour Relations Act shall apply as if the employee was performing such functions in the territory of their home country

d) shall not be liable for any damage or loss caused to anyone while exercising any power or performing any duty in terms of the OSBP Act or any failure to exercise a power or perform a duty under the OSBP Act.

General principles relating to labour relations and conditions of employment should find expression in the OSBP legislation and bilateral agreement.

6.5 Simplification and harmonisation of procedures

6.5.1 Introduction

A border post is a space where the border laws, administration and systems of two countries interact with one another and with many international and regional regulatory regimes. Bodies such as the WTO, the World Customs Union, the AU and SADC promote enabling economic development by simplifying and harmonising regional laws, processes, systems and procedures. South Africa is a member of all these bodies and has endorsed policy positions held by these bodies, as articulated in various international agreements.

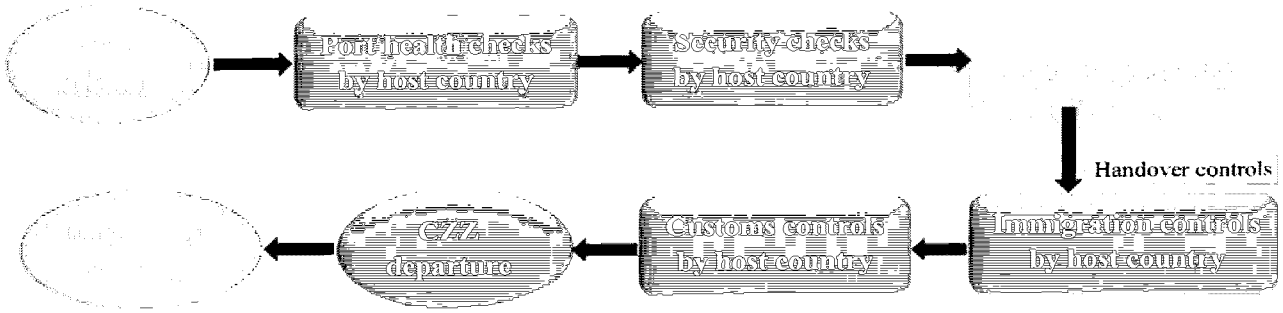
Establishing an OSBP as a bilateral project supported by multiple stakeholders, provides a platform for both countries to cooperate and take the necessary steps to simplify and harmonise their processes and system. Border crossing procedures under the OSBP framework differ from operations at traditional two-stop border posts, although the role of each agency generally remains. Simplifying and harmonising operational procedures and joint controls are cornerstones of OSBP operations.

The core objective of any border modernisation programme, including OSBPs, is to introduce streamlined and harmonised procedures that take advantage of the various tools available to achieve a good balance between the required controls, and facilitating trade and the movement of people. It is often easier to start with the construction of infrastructure than with developing procedures and systems. There have been many examples of this approach in Africa. However, designing buildings, negotiating a legal framework, and reviewing ICT systems without a consensus on new procedures will not result in effective OSBPs.

Establishing OSBPs requires streamlining and harmonising border crossing procedures for people, goods and conveyances. Thus, extending the application of border procedures applied under the traditional two-stop framework to an OSBP framework without simplifying and harmonising them undermines efforts to reduce the time spent at a border and the associated

costs and security threats. Border crossings are logistics points along integrated international supply chains that can easily become unnecessary movement control bottlenecks if processes are not simplified, streamlined and harmonised. This section deals with the simplifying, streamlining and harmonising border controls to process the movement of persons, goods and conveyances as depicted in **Figure 6.1** below. The general principle that applies in the processing of all movements is that all the controls of the adjoining country should be completed before any control of the hosting country can commence.

Figure 6.1: The general process flow at the CCZ



6.5.2 Harmonising and simplifying border procedures related to the movement of persons

Travellers and traders should complete the requirements of the country they are leaving before seeking permission to enter the next country. The principal legislation that regulates the cross-border movement of persons in South Africa is the Immigration Act 13 of 2002, which is administered by the DHA. Arrival and departure controls are outlined in this Act. For instance, every person who intends to visit the country must have a valid passport, a visa and must comply with the entry requirements prescribed.

Another pertinent legislation is the National Health Act 61 of 2003. This Act establishes the port health function within the border environment. Port health plays an important role in protecting human health by preventing the international spread of communicable diseases through South African PoEs and monitoring the import of health-related goods. The port health service is defined as the first line of defence to protect the citizens of South Africa and visitors against the health risks associated with the cross-border movement of people, conveyances, baggage, cargo, shipments and other imported consignments.

At the traditional two-stop border posts, the immigration and port health controls are repeated on both sides of the border. At the OSBP, these controls will still be undertaken twice but on one side of the border. That is, the processes will take place at the entry country in the CCZ. The best practice for exercising port health functions at any PoE is that it should be the first border processing formality that all travellers, traders and conveyances encounter. Within an

OSBP, this could take various forms. Either the port health function can be the first border formality to be jointly exercised by both South Africa and the neighbouring country at a location to be determined by both parties, or it is the first function to be performed respectively during the exit and entry procedures of the two countries.

Other important legislation that regulates the cross-border movement of persons is the Refugees Act 130 of 1998. A person who is fleeing from the fear of persecution from the exit State will be dealt with as prescribed in the Refugees Act.

The cross-border movement of persons through the OSBPs consider the standards and protocols derived from the customary international law and regional and international agreements that have been either signed or ratified by each State.

In order to eliminate red tape and duplication of processes, the following standards will be institutionalised and spelt out in detail in the OSBP manual:

Technology-enabled fast-track clearance system for the movement of persons

Generally, the cross-border movement of persons through the PoEs includes the following legitimate categories:

- Citizens and permanent residents
- Visitors or tourists
- Traders or business persons
- Students and academics
- Migrant workers
- Asylum seekers and refugees.

Low-risk travellers including citizens and permanent residents of OSBP partner States, frequent visitors and businesspersons will qualify to apply for enrolment in the fast-track automated clearance system. Key elements of the system are summarised below:

- Automated e-passport gates: e-passport gates are automated self-service booths or mobile device that will be located at immigration checkpoints in each CCZ.
- Frequent traveller programme: the programme will allow eligible travellers to enjoy convenient immigration clearance via automated clearance facilities. Services will include fast-tracking frequent travellers such as truck and bus drivers, businesspersons, and tourists. Border officers will need only to check that the travellers are the authorised holders of the written authority. Border processes that still need to be undertaken at border crossings should be informed by risk and kept to the minimum.

- Long-term multiple entry visa: this visa will be available to eligible frequent travellers including businesspersons, students and academics who do not have long-term residence authority in the host country. It is preferable that the two countries agree on the categories of frequent travellers.

Frequent travellers who would like to apply for enrolment to the fast-track clearance system should apply at any location determined by each State. SA regards the fast-track clearance as a fundamental principle that must be operationalised at the OSBP to enable seamless movement of people. Parameters and criteria within which the fast-track service will operate will be agreed by both countries.

The design of the clearance process for cross-border movement of persons at the OSBP should consider various means of transport:

- Clearance of pedestrians, and passengers, drivers and crew using public transport
- Clearance of passengers using private transport
- Clearance of drivers and crew of freight vehicles.

The general principle that should be embedded in the bilateral agreement and procedures manual is that the traveller's clearance is only completed after all exit and entry controls have been satisfied. That is, a traveller who has been cleared to exit the adjoining State by immigration officers may still be refused departure if other controls related to, *inter alia,* goods and conveyance, are not met. Equally, a traveller who has been cleared to enter the host State by immigration officers may still be refused entry if other controls related to, *inter alia,* goods and conveyance, are not met.

Granting/refusing leave to enter

Both countries operating within an OSBP examine travellers according to their respective immigration laws and policies. Where travellers do not qualify for leave to enter, they should be refused entry and returned to the officers of the country of departure. The country of departure cannot refuse to accept travellers who have been refused entry to the country of entry. However, South Africa will not refuse its citizens the right to enter as this will be tantamount to breaking the Constitution. The reciprocity principle, which contends that the OSBP partner State will not refuse entry to its citizens, is a fundamental principle that must be embedded in the bilateral agreements.

The country of departure will retain the responsibility to readmit the person (either a person claiming to be a citizen or a third country national) if the person is refused entry by the country of arrival. Reasons for non-admissibility by the receiving country could be on the grounds of identity theft or fraud or any other inadmissibility grounds.

6.5.3 Harmonising and simplifying border procedures related to the movement of goods

Regarding the process of simplifying and harmonising border procedures, the Revised Kyoto Convention (RKC), effective from 3 February 2006, provides international standards and recommended practices for modern customs procedures and techniques. The RKC supports trade facilitation and effective controls through the use of simple efficient customs procedures. It is mandatory for all contracting parties of the World Customs Organization to accept its obligatory rules. The key principles of the RKC are as follows:

- Transparency and predictability of customs actions
- Standardisation and simplification of the goods declaration and supporting documents
- Simplified procedures for authorised persons
- Maximum use of information technology
- Minimum necessary customs control to ensure compliance with regulations
- Use of risk management and audit-based controls
- Coordinated interventions with other border agencies
- Partnership with trade.

The legislation that regulates the cross-border movement of goods in South Africa is the Customs Control Act 31 of 2014[9]. The Customs Control Act already makes provision for customs services in an OSBP setup.

The following customs principles will be observed at the OSBP:

- Exit formalities to be completed before entry formalities may start and customs jurisdiction moves from the country of exit to the country of entry once exit formalities are completed.
- Only the country of exit customs officials may stop, seize or detain persons, goods or conveyances in the control zone for any customs or mandated contraventions until exit formalities are completed.
- Only the country of entry customs officials may stop, seize or detain persons, goods or conveyances in the control zone for any customs or mandated contraventions once entry formalities have started.
- Article 5.2 of the WTO Trade Facilitation Agreement requires members to inform the carrier or importer promptly when goods declared for importation are detained for inspection.

[9] The Act has not yet been gazetted for implementation and is still dependent on the finalisation of the regulations.

- Respective customs administrations would have to jointly develop proposed customs solutions and deployment, which could include joint inspections, including inspections on each other's behalf, etc.

The following standards will be applicable at the OSBP and should be spelt out in detail in the OSBP manual:

Electronic single window systems

The electronic single window system is an international standard or good/best practice that enables cross-border traders to submit relevant documents at a single location and/or through a single entity. A definition of a single window is "a facility that allows parties involved in trade and transport to lodge standardised information and documents with a single-entry point to fulfil all import, export, and transit-related regulatory requirements." The OSBP Act will make provision for establishing the single window system that will enable cross-border travellers and traders to lodge relevant documents at a single platform. An accreditation system should be in place where those who meet the criteria of a trusted traveller and traders are fast-tracked because they completed part of the preclearance process.

Preclearance and fast-track

Preclearance processing is a critical element of the single window system that enables importers and exporters, through their clearing agents, to submit trade documents to border agencies prior to the arrival of goods at a point of clearance. Preclearance processing provides sufficient time for border agencies to examine documents thoroughly and to allocate appropriate resources and a risk rating in anticipation of the arrival of the goods. A customs administration requires traders to put their pre-cleared goods under its physical control to ensure the collection of the import duties and taxes, prevention of the contraband smuggling, and execution of all trade-related laws and regulations.

Many customs administrations prefer traders and clearing agents to lodge a declaration prior to arrival under a pre-arrival lodgement scheme, but they cannot release goods before the physical arrival at the border post is confirmed. The OSBP concept is based on the principle that systems (back and front office) and officials can be put in place to allow 80% or more of cases to be fast-tracked while actively managing risk. An important element of any OSBP operating model must be to enable a pre-arrival clearance system involving pre-lodgement and pre-registration of documents. This could be linked to online systems such as those established by Sars. All preclearance systems require another area to be simplified, harmonised and strengthened: controls related to risk management. This should include simplifying and improving policing and border control enforcement procedures to raise the level of security. A related step is to make these procedures known to key stakeholders including logistics agents and local communities.

To make the OSBPs agile and sterile, the preclearance requirement must be embedded in the OSBP Act and bilateral agreements. It should apply reciprocally; that is, conveyances carrying commercial goods should not be granted right to approach an OSBP unless they have met

CONTINUES ON PAGE 130 - PART 2

Vol. 666 31 December Desember 2020 No. 44048

PART 2 OF 3

preclearance requirements. Should a conveyance approach an OSBP without a preclearance certificate, the operator or owner of the conveyance should be subjected to a fine or levy.

Cross-border clearing agents

Cross-border agents play an important role in facilitating trade and, in some countries, are an essential part of the cross-border movement systems for goods and conveyances. In designing an OSBP, the two countries must agree on the extent to which cross-border clearing agents can have access to the OSBP and areas such as CCZs.

Ideally, to maintain acceptable levels of security the CCZ should be sterile and, in upgrading the procedures and systems, a solution must be found that allows the clearing agents to play their necessary role without compromising security. The general principle is for as many of the procedures to be completed as possible before the freight arrives at the port and for the necessary data to be made available in real time. In principle, clearing agents should not be allowed to operate within the OSBP: that is, they should not have physical offices at the OSBP.

6.5.4 Harmonising and simplifying border procedures related to the movement of conveyances

The primary legislation that regulates the cross-border movement of conveyances (public and commercial conveyances) through the PoE in South Africa is the Cross Border Road Transport Act 4 of 1998. The Act provides for cooperative and coordinated advice, regulation, facilitation and law enforcement in respect of cross-border road transport by the public and private sectors. Section 25(1) of the Act states that no person may undertake cross-border road transport unless they are the holder of a permit.

The Act also provides for establishing the CBRTA, which is responsible for issuing permits to cross-border road transport operators. The agency exists primarily to regulate and administer cross-border road transport permits. It is responsible for regulating access to the cross-border road transport market, freight and passengers, through a permit administration regime. The CBRTA is also tasked with ensuring that operators comply with cross-border regulations, as well as the provisions of the bi- and multilateral road transport agreements. The following principles for clearing conveyances will be observed at the OSBP:

- Promote seamless cross-border flow of commercial freight and passenger transport between South Africa and SADC countries by road
- Remove impediments that constrain the flow of passengers and goods across the border
- Reduce operational constraints that have a negative impact on the cross-border road transport industry
- Liberalise market access for freight transport operators

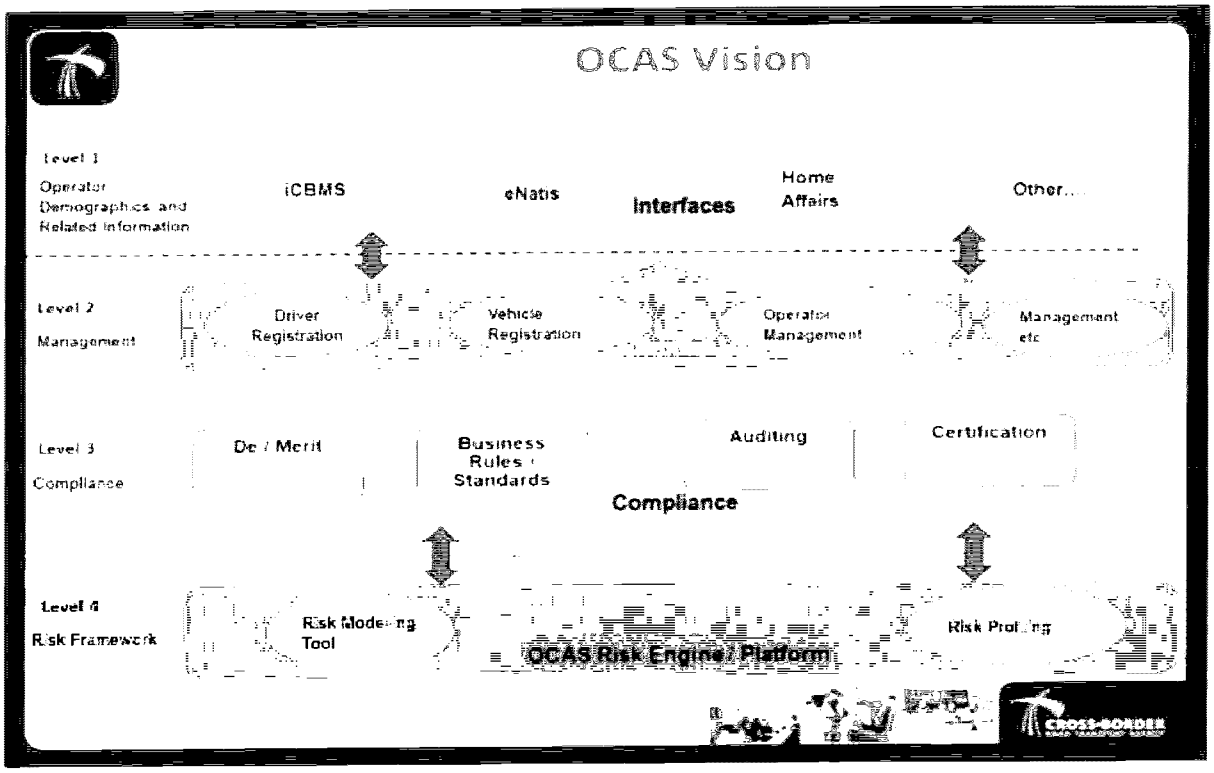
- Mutually recognise licences and permits by CBRT administration of respective SADC countries
- Adopt a predetermined risk-profiling system to separate compliant from non-compliant operators
- Enhance road safety and reduce accidents and fatalities on the roads.

Respective cross-border road transport administrations of the OSBP states would have to jointly develop risk-profiling systems, which could include joint fast-tracking inspections, including inspections on each other's behalf. There could be instances, however, where South Africa would want to develop and implement its own risk-profiling and risk management systems to address cross-border road transport challenges. The risk-profiling system should rank operators as either low-risk, medium-risk or high-risk. Low-risk operators or preferred operators should qualify to apply for advance or fast-track clearance at a PoE. Parameters and criteria within which the fast-track service will operate will be agreed by both countries. The CBRTA is in the process of introducing the Operator Compliance Certification Scheme (OCAS) or tool. The OCAS is an intelligent risk-based regulatory tool for certifying and licencing cross-border operators. It is a tool for implementing the requirements of ISO/SANS 39001 Road Traffic Safety Management Systems and the Multilateral Cross-Border Road Transport Agreement or the Tripartite Transport Transit Facilitation Programme.

OCAS recognises the requirements and interface requirements in terms of the various components of OCAS, the Cross-Border Road Transport Management System, other border management systems, other road transport and traffic information systems in South Africa, requirements for the ISO 39001 (Road Traffic Safety Management Systems) and the Tripartite Transport Transit Facilitation Programme / Multilateral Cross-Border Road Transport Agreement.

OCAS shall integrate national road transport systems and enable an interface to road transport systems at a regional level. **Figure 6.2** below demonstrates how the OCAS system interfaces with the road transport information systems.

Figure 6.2: OCAS system interface with road transport information systems



OCAS will be introduced as a cross-border road transport quality regulatory tool (accreditation tool) in the tripartite member states. It will be mandatory for all cross-border operators e.g. South Africa's and counterparts, and preferential treatment at the border posts will be given according to their level of compliance (1-star; 3-star; and 5-star). A cross-border permit (freight, passenger and tourist) will be a requirement at border posts. This will primarily show the vehicle that crossed the border (inbound and outbound) with its respective driver. Preclearance of passengers and cross-border passenger vehicles by the relevant border post before they leave the point of origin (dedicated ranking facility), will help to eliminate encroaching illegal ranking facilities and piracy.

6.6 ICT and data exchange

6.6.1 Introduction

This section deals with the policy and strategic issues relating to ICT and the exchange of data and information. Data and information are essential for a modernised OSBP to function efficiently and effectively. All border controls involve receiving and updating digital data and information. Harmonising and simplifying the processes depend on the exchange of data and information.

OSBP methodology works on a risk management principle that is data dependent. For instance, once a vehicle has stopped, the health and biohazard inspectors would arrive as pre-scheduled on the system, which requires a management system that runs on real-time data. Risks must continually be assessed using data so that, if necessary, a vehicle could be moved into the exceptions channel. The system would require those at ports to be securely connected to back office hubs with risk engines that integrate data from different sources. This requires policy, legislation and institutions as prescribed by the Protection of Personal Information Act 4 of 2013 (POPIA) and other relevant laws to be in place, implemented and enforced to protect constitutional rights such as privacy, transparency, fairness and security. Relevant information may be exchanged regarding persons, goods, and vehicles; however, this will need to be mutually agreed by the OSBP partner States.

6.6.2 Collecting and sharing traveller information

Collecting traveller information can be time-consuming at an OSBP as the traveller has to provide their information twice. Using interoperable systems will enable countries implementing an OSBP to explore the possibility of requiring travellers to provide their information only once, with the results transmitted to both countries. However, for each country minimum standards and security considerations will be built into the system.

Immigration officers at a PoE in South Africa collect a wealth of traveller information that is stored in the DHA Enhanced Movement Control System, which contains a record of the cross-border movement of every person. That record contains information gathered at every movement: the time, date and PoE, and the information taken from their travel documents such as passports, photos and, in some cases, fingerprints.

The DHA does not automatically share this information with other organs of state and international bodies such as the International Criminal Police Organization (Interpol). However, there are procedures and agreements in place that enable some information sharing, spreading the information beyond just the DHA's control. A similar arrangement will be put in place at the OSBP. Collecting and sharing traveller information will be guided by national policy frameworks. In South Africa, the POPIA sets strict conditions under which personal information held by the State could be shared with a third party. Due regard for the POPIA, the purpose of the information, the security of information and the security of the system will be considered when deciding on the nature of personal information that can be shared.

South Africa is in the process of modernising its identity management systems. The common feature of this process is collecting biometric data from all persons that visit or reside in the country. Key developments include replacing the Enhanced Movement Control System with the Biometric Movement Control System, and replacing the Home Affairs National Identification System with the Automated Biometric Identification System.

The introduction of POPIA, the Biometric Movement Control System and Automated Biometric Identification System will inform South Africa's position on collecting and sharing

the traveller's personal information with the OSBP partner State. Only sharing general and not personal information could be allowed, on condition that information shared will not compromise the traveller's privacy, health, security, economic wellbeing, etc.

6.6.3 Collection and sharing of freight information

For "smart" logistics corridors and near-future OSBPs to operate, the data or information from weigh bridges, seals on containers, car number plates, etc., are transmitted in real time to be analysed. In the longer term, the plan is to have no-stop border posts for most traffic where officials will monitor for risks, investigate exceptions, and continually improve the services and systems. This requires robust policy, legislation and institutions to enforce common standards to purchase and develop ICT that enables interfaces and other aspects of interoperability.

6.6.4 Technology-enabled OSBPs

The OSBP Sourcebook (2016) makes a critical observation regarding the approach that should be adopted to modernise OSBPs and enable seamless movement of persons, goods and conveyances. "ICT is a critical component of collaborative single window systems, simplification of documentation, border management, and modernisation of customs, immigration, and related services. The increase in the number of travellers along with increases in volumes of vehicular traffic and cargo at borders requires a strategic balance between controls and facilitation. ICT allows for the efficient use of limited resources to manage borders by facilitating intra/interconnectivity of agencies while promoting the exchange of data, which is vital for implementing risk management systems and for understanding mobility and trade patterns."

Once the policy and legal frameworks are largely in place, an ICT and data and information exchange strategy must be agreed at national and then bilateral levels. The first phase could be to digitise the core processes that would make the largest impact on the efficiency of trade. Using a single window approach, there could be interfaces between systems and the necessary data or information shared. For instance, a driver, freight and truck can be processed at one location with officials having access to all relevant information.

One potential benefit of technology-enabled OSBPs is that both countries would move towards integration with the emerging global economy.

6.6.5 Border connectivity to national headquarters

While the head offices of border agencies rely on information obtained from each of the country's borders, in many instances the ICT connections are weak and data or information is transferred manually. The lack of connections, or slow systems, reduces productivity and is a

major problem in many border environments. There is an urgent need to develop an ICT system that will establish an interface with national systems for providing pre-arrival information. In this case, subject to risk management criteria, the freight may be pre-cleared or prioritised for clearance, leading to much faster clearance and release.

6.6.6 Common control zone connectivity

One of the basic elements supporting the effectiveness of the border services in the CCZ of an OSBP is the availability of a modern ICT network. This is more so in a juxtaposed OSBP where exit controls are carried out in separate facilities and the lack of connectivity may cause officers to revert to manual procedures and then enter data into the agency computer system later, with a consequent adverse impact on productivity and security. The entire CCZ needs to be technology-enabled.

The ICT system employed for CCZ connectivity should:

a. have a central database generating alerts that provide real-time data or information on the cross-border movements
b. have an efficient and timely system for collecting, processing, and sharing data and information on all border activities
c. enable automated information exchange between countries on agreed data and information
d. ensure cryptographic security
e. ensure interfaced electronic systems with the OSBP partner States
f. enable authorised users' real-time access to specific data sources.

6.6.7 Essential enablers of ICT technology and data and information exchange

All the functions at a PoE depend on digital processes being secure. Without adequate security for the ICT infrastructure, ICT becomes a risk and not an asset. Therefore, the ICT infrastructure used in the control zone must meet the Minimum Information Security Standards. This is a standard for the minimum information security measures that any institution must put in place for sensitive or classified information, to protect national security.

A critical enabler for OSBP modernisation and connectivity is the adoption, monitoring and enforcement of common ICT and data transfer and information standards and rules. Such standards and rules must be agreed between the OSBP partner States and should be embedded in the bilateral agreements. Another critical enabler would be the ICT infrastructure in the form of networks that must be an integral part of the OSBP design, including mapping present and future equipment and workstations.

In the context of the 4IR, the same security systems would enable:

- risks to be managed and safety and security enhanced
- essential and reliable data and information to be generated in real time
- greater efficiency by rapidly facilitating low-risk transactions
- secure interfaces with OSBP partner countries.

Expanding digital platforms with a growing user base will require systemically managing risks by putting in place a security system that includes cyber security. An effective system must be able to continually monitor the ICT systems. The Cyber Security Bill currently before the legislature will establish security processes, standards and structures that would guide the design of the cyber security measures required, and provisions for backing up data and business continuity.

Finally, the DHA is currently developing a business case for a National Targeting Centre (NTC) for the border environment in South Africa. The NTC is envisaged as a centralised technology, information and data hub for the South African border environment with a central focus on identifying and mitigating border-related risks. The NTC will be a crucial ICT and intelligence enabler for the efficient functioning of OSBPs.

6.7 Infrastructure and facilities

6.7.1 Introduction

The purpose of OSBP infrastructure is to facilitate the rapid, secure and seamless movement of people, goods and conveyances through a PoE in accordance with the rights and standards set out in a bilateral agreement and the applicable domestic laws of each country.

When modernising a commercial PoE and implementing OSBP methodology, the State must invest considerable resources. **The design must be fit for purpose and based on an objective cost-benefit and risk analysis.** Underlying the three "OSBP models" is a standard model based on the principles of applying harmonised procedures and systems at one location to a differentiated flow of traffic. High-risk traffic is diverted to an alternative process for further investigation and a decision while low-risk traffic proceeds. The following principles must be applied to the design of OSBP physical infrastructure (roads and buildings) and soft infrastructure (facilities, networks, equipment).

6.7.2 OSBP design principles

The infrastructure design must be fit for purpose and cost effective, taking account of:

a) the foundational principles of the OSBP as outlined earlier in the document

b) the location of the OSBP, on a strategic logistics corridor and being connected to core functions and systems of the State and the economy

c) the physical terrain, topography, environmental considerations and any other natural features or constraints at the OSBP

d) the OSBP laws and standards of both countries, in the region and at a global level

e) the ratified bilateral agreement.

Given trends in port and corridor use, and the uncertain and dynamic nature of changes that are already happening, the following infrastructure design principles must formally be adopted. Infrastructure design and planning for implementation must allow for:

a) a phased approach to replacing functions performed at the ports with preclearance through online platforms, which will have an impact on roads, buildings and the use of space

b) unpredictable changes in the patterns and volumes of trade, the nature and use of conveyances and the development of smart, flexible logistics systems

c) vehicular traffic segmentation through the port

d) the central importance of generating, using and networking data

e) the need to maintain high security and sterility in physical and digital security standards, including in designated zones

f) the need to limit high-cost hard infrastructure and shift funds strategically to sustainable and environmentally-friendly modular design, smart facilities, networks, systems development and training at the ports and at corridor, back office and national levels.

6.7.3 Design standards and harmonisation

Harmonising physical designs could provide a user-friendly approach by eliminating confusion regarding flows at the CCZ. However, facility requirements are not necessarily symmetrical as the required capacity may differ by traffic direction. Given that different designers may be involved on opposite sides of an OSBP, close coordination between both sides is likely to be necessary to maintain a certain level of harmonisation in design and standards.

Selection of facility components

OSBPs may include a number of facility components that can be categorised by function:

a) cargo clearance facilities

b) vehicle inspection facilities

c) scanning facilities

d) incineration and short-term quarantine facilities

e) passenger clearance, interviewing and holding facilitics

f) administrative facilities

g) supporting services.

Core facility components are those required for every OSBP, which should be developed in the initial development phase, while others are optional facilities depending on the size or characteristics of the OSBP. Facility components should be selected by examining such OSBP characteristics as well as the requirements to realise procedures agreed by the adjoining countries. The following sections detail each component.

Segregation and segmentation of traffic flows

If OSBPs are to be efficient, the traffic flow and physical facilities must be planned to save time and provide for traffic moving quickly through the facility. Generally, passenger and freight traffic should be segmented and separate parking areas provided. Travellers can generally be cleared much faster and should be expedited through the facility in dedicated lanes, channels or parts of the building and traffic patterns. Where heavy volumes of passenger traffic are handled, the design should provide for clearing vehicles in lanes.

This principle of traffic segmentation in the OSBP requires design creativity that balances security with the efficiency of port operations. The OSBP design should make provision for, *inter alia*, dedicated lanes, facilities and/or parking bays that cater for:

- private passenger vehicles
- public transportation, such as buses and taxis
- hazardous cargo and abnormal freight
- VIP and diplomatic vehicles and travellers
- trusted travellers, traders and conveyances
- specialised inspection bays
- general avoidance of cross-contamination of different types of traffic flows and movement
- separation of entry and exit traffic flows.

Processing requirements

The types of processing affect traffic flow through the facility, parking requirements, and facility design. Identifying the predominant types of cargo and projections for growth or

decline must be considered in the OSBP facilities' design. The use of scanning and inspections is also a major consideration in planning for traffic lanes and parking within the facilities. Unless properly situated, they can cause considerable congestion in the CCZ or force an awkward traffic flow.

Secondary inspection areas must also be provided for vehicles in a manner that will not impede or obstruct the dominant flows of traffic through the port.

Chapter 7: Enabling legal framework

7.1 Introduction

Border controls involve various functions performed by officers from different government organisations using the specific authority granted in a State's national laws. It is necessary for the officers' functions and powers to be authorised in law as they potentially entail a limitation of the rights of persons. These functions are the expression of the sovereign power and therefore cannot be privatised.

The OSBP concept envisaged for any PoE requires legal authority beyond that which is provided by current legislation for two reasons. Firstly, it will entail various officers of one State performing border controls in terms of its national laws extraterritorially in another State. Secondly, a legal mandate is required for arrangements to host a State's border control officers where they operate in terms of their own national laws within the territory of another State.

This chapter provides an outline of the legislative framework and instruments necessary to establish and maintain OSBPs.

7.2 An OSBP Act

As discussed in the preceding chapters, an OSBP Act is required to put the OSBP concept into operation. The following headings indicate the possible main elements of an OSBP Act:

i) Objective for the establishment of the OSBP

ii) **Definitions:** it is important that all definitions and any statements of purpose are clear and aligned to policy.

iii) **Foundational principles:** these principles are discussed in Chapter 4 and are non-negotiable.

iv) **Establishing the OSBP:** the geographic area of the OSBP and related zones (CCZ and EUZ) must be clearly demarcated and stated in the respective OSBP Acts and bilateral agreement.

v) **Competent government authority:** for negotiating agreements with one or more adjoining states. Each State must designate a single national authority to negotiate an agreement and any subsidiary annexes or memorandums of understanding. The BMA has been designated as the competent government authority in South Africa.

vi) **Extraterritorial application:** of the legislation of the parties to the OSBP agreements. The application must cover both South African officials and officials of the other party. This is discussed in Chapter 6, which deals with the challenge extraterritorially may present and suggests an approach to ensure laws comply with the Constitution.

vii) **Determining jurisdiction**: including establishing and delimiting physical and soft infrastructure of the OSBP. These will have to be carefully specified in the Act or regulations together with the roles of states, and functions and roles of respective officials. The models of OSBP discussed in Chapter 4 has an impact on the nature and extent of extraterritoriality that may have to be specified in the Act.

viii) **Applying criminal law in relation to the OSBP:** an OSBP is a highly regulated environment and ensuring adequate enforcement by both parties is fundamental to its success. A policy framework on applying criminal law is dealt with in Chapter 6.

ix) **Schedule of national laws that must be extraterritorially applicable**: this is based on a review of legislation of both countries.

x) **Responsibility and financing for shared facilities:** equitable sharing of responsibility and costs for shared facilities must be clearly stated in the respective OSBP Acts and bilateral agreement.

xi) **Disputes between OSBP partner States:** escalation and conflict resolution procedures must be clearly stated in the respective OSBP Acts and bilateral agreement.

xii) **Provision for emergencies**: examples are a natural disaster or terrorist attack, in which case the security services of one or both countries would have to intervene and rules and procedures must be clearly stated in the respective OSBP Acts and bilateral agreement.

xiii) **Provision for regulations**: given the nature of the legislation and the need for long-term management of agreements and other factors, there will be a need for regulations.

7.3 Changes to existing legislation

Key functions pertaining to immigration, customs, public health, phytosanitary and environmental inspections, cross-border public transportation and biosecurity will need to be assessed in relevant pieces of legislation. Additionally, the laws that impact directly on core OSBP processes must be reviewed and may be repealed or amended, where necessary, to provide for executing associated border services extraterritorially:

a. BMA Act 2 of 2020
b. Immigration Act 13 of 2002
c. Customs Control Act 31 of 2014
d. National Health Act 61 of 2003
e. Agricultural Pests Act 36 of 1983

f. Cross Border Road Transport Act 4 of 1998.

This list is not exhaustive. A separate legislative and regulatory audit will need to be done when drafting the OSBP legislation. Each department will take full responsibility for making necessary policy and legal changes. Coordination and oversight would be the responsibility of the BMA as the lead agency for establishing the OSBP.

7.4 The OSBP bilateral agreement

The OSBP bilateral agreement is a legal instrument that is key to ensuring that two states cooperate and succeed in establishing a sustainable OSBP. A viable agreement will be comprehensive, well-defined and have a solid policy and legislative foundation. The following principles should guide the drafting of an OSBP bilateral agreement.

a. A bilateral OSBP agreement is negotiated and signed by the authorised ministers of two countries, supported by their respective technical teams. The agreement only comes into force after ratification by both countries.

b. South Africa should have an OSBP policy in place to guide OSBP bilateral negotiations, and legislation in the form of an OSBP Act. The minster of home affairs would be designated as the lead authority in OSBP negotiations.

c. An OSBP agreement or its annexes must have a schedule identifying applicable legislation and the relevant authorities.

d. The minimum list of border functions to be addressed in the bilateral agreement include:

   i) Customs and revenue
   ii) Immigration
   iii) National security
   iv) Border policing
   v) Agriculture
   vi) Food, animal and plant inspection
   vii) Public health
   viii) Biosecurity
   ix) Public transport
   x) Environment management inspections
   xi) Other relevant border functions.

The OSBP bilateral agreement must provide for developing an OSBP procedures manual and guidelines, and provide for institutional arrangements to manage the OSBP.

Chapter 8: Governance and institutional arrangements

8.1 Policy principles

Good governance is essential for the sustainability and success of OSBP programmes and projects. A national OSBP policy must reflect a commitment to good governance as demanded in the Constitution. This requires an explicit OSBP governance policy and institutionalising the policy through establishing and maintaining appropriately accountable and resourced governance structures.

The King IV report sets out the general principles:

> "The role of the governing body is to lead the organisation through the discharge of its responsibilities in relation to strategic direction, policy approval, oversight and accountability such that the good governance outcomes of an ethical culture, good performance, effective control and legitimacy with stakeholders are achieved by the organisation."

The King IV report and other governance codes increasingly emphasise sustainable development and good stewardship being recognised as an essential resource. A country invests in an OSBP with the expectation that it will be maintained for at least 15 – 20 years, which requires governance processes to be institutionalised at bilateral and national levels.

The overall OSBP institutional arrangements should provide for multilevel governance modalities that will be formalised across the strategic, operational and tactical levels between and within the OSBP partner States. Key principles that should inform the multilevel governance arrangements are:

- Transparency
- Public participation
- Accountability
- Subsidiarity
- Co-responsibility
- Rule of law
- Respect for fundamental human rights
- Mutual respect for the sovereignty of the partner States

Various governance structures will need to be established at various levels to oversee and manage functions at the OSBP. This could include:

i) A ministerial committee that will exercise political oversight

ii) A steering committee that will be supported by relevant technical committees or working groups

iii) Technical committees / TWGs that will be responsible for executing the work programme and all technical activities

iv) A joint border operations committee as a local committee based at the border post.

The principle and value of good governance is foundational in the South African Constitution. The challenge is how to ensure that the importance of governance and governance institutions is explicitly recognised in bilateral OSBP agreements and other relevant policy and legal instruments, and to establish and maintain strong governance institutions at a national level in South Africa.

The OSBP Act should specify the lead authority and lead agency responsible for OSBP governance; and in some countries it should also establish a national OSBP oversight structure. In South Africa, the BMA, with the support of other relevant organs of State, will be the lead agency responsible for managing the OSBP.

8.2 Political commitment

Political commitment is critical to the success of any OSBP. The political considerations are whether South Africa's neighbours are as politically committed to making the OSBPs work as South Africa is. To be successfully implemented, the OSBP framework must involve not only considerable changes in how border agencies work with each other in one country, but also complete cooperation between the border agencies of two countries.

The effort required to implement an OSBP does not end at the official opening. Border improvements are an ongoing process that should continue with an active development plan led by the lead agency, ministry or department, which in the case of South Africa, is the DHA. In future, the BMA will assume operational responsibility for PoE infrastructure and maintenance making the OSBP, and the estate, easier to manage.

8.3 Joint technical working group

A joint TWG, comprising senior technical officials from South Africa and the adjoining country where an OSBP is to be introduced, must be established.

The TWG will be made up of representatives from all the border agencies operating at the border. The chair and the host of the TWG meetings and workshops should be rotated between the two countries and each country, in principle, should meet the cost of participating in the activities to develop procedures unless agreed otherwise.

Chapter 9: OSBP implementation framework

9.1 Introduction

In its effort to develop a well-researched and extensively consulted policy document, the DHA engaged with various stakeholders that have an interest in effectively and efficiently managing the PoEs. Most entities that operate in the border environment were also consulted through an interdepartmental OSBP steering committee that was established to oversee the establishment of the OSBPs.

Technical consultations at a regional level were also undertaken through study tours to the Chirundu (Zimbabwe and Zambia) and Namanga (Tanzania and Kenya) border posts. Additional technical binational meetings were held with neighbouring countries (Namibia, Lesotho, Botswana, Mozambique, Eswatini and Zimbabwe) on redeveloping the six land PoEs as OSBPs, the OSBP policy and, in particular, the preferred OSBP model. Most of the neighbouring countries prefer a juxtaposed model.

The minister of home affairs has also consulted with, and met, his counterparts from Botswana, Lesotho, eSwatini, Zimbabwe and Mozambique. They discussed, *inter alia*, the project of redeveloping the six land PoEs as OSBPs and improving border movement operations. All these countries support the concept of establishing OSBPs between South Africa and their countries.

9.2 Business case and baseline survey

A full OSBP business case will be prepared to assess the feasibility, benefits, costs, etc. of a proposed OSBP. This business case will address, *inter alia*, the rationale, feasibility, preconditions and cost-benefit analysis of establishing an OSBP, and will also include a baseline survey. A baseline survey will be carried out for every border that is to be transformed into an OSBP. The baseline survey will be used to assess the situation prevailing at both borders that are to be merged into an OSBP before any activities start. Information that should be collected includes the traffic using the border posts (both ways), disaggregated as much as possible (passenger vehicles, small buses, medium buses, long-distance coaches, container carriers, break-bulk, refrigerated, tankers, etc.), and the average time taken to clear the borders for each class of vehicle (upper and lower limits). This information will be used to project traffic flows for the following 10 – 20 years so that the design for the OSBP is able to accommodate this traffic.

A baseline will detail the processes followed by all border agencies on both sides of the border for entry and exit procedures. These processes are used as the basis for mapping the standard operating procedures to ensure that no processes are omitted. A baseline will detail the infrastructure that is in place, which will be used to plan the new infrastructure required. The baseline will also itemise the computerised systems in place and the ICT and telephony hardware. This information will assist to perform an ICT software and hardware gap analysis.

9.3 Design the physical facilities as a common integrated facility

Physical facilities will be designed according to the planned procedures to allow for a logical and smooth movement of vehicles, persons and documents at the border post. The approach to infrastructure development at borders will be "minimalist" when they are converted from two-stop borders to OSBPs. This is to encourage the completion of as many of the clearance processes as possible behind the border and to discourage delays at the border, simply because the infrastructure is in place and should be used.

South Africa and the adjoining State shall each provide comparable office space and accommodation for the other, within the facilities located in the host State, and waive all costs related to the occupation and maintenance of such premises. Both states should offer utilities on a reciprocal basis to the adjoining State. South Africa and the adjoining State should harmonise the structures and facilities in the control zones to mirror each other, using coordinated designs and procuring related construction, maintenance and management services. In doing so, the states will consult both internal and external public and private sector stakeholders for input on their requirements in the control zones.

9.4 Institutional arrangements

The appointment of a lead agency is important to the success of OSBP operations. Whereas South Africa already has a BMA (BMA Act), the neighbouring states with which South Africa wishes to establish OSBPs will be encouraged to appoint a lead agency to coordinate OSBP preparatory and post-implementation activities. However, the choice of a lead agency by any country should be purely based on national considerations.

9.5 Financial implications

In 2015, the DHA obtained approval from the National Treasury to register the project as a public-private partnership. This has led to the DHA implementing the public-private partnership project to redevelop six land PoEs as OSBPs. The proposed funding model for the public-private partnership project will be a 20-year concession entered into with multiple successful private parties to redevelop and maintain key facilities and infrastructure at the identified land PoEs. A draft request for proposals tender document is being prepared and will be submitted to the National Treasury for approval and subsequent issuing to the market. The funding model for the OSBP will be based on a user-pay principle. The DHA has undertaken two targeted interactions with commercial users who indicated satisfaction with the principle of introducing commercial user fees on condition that port processing times would be reduced with greater efficiencies.

9.6 Change management

The start of joint border operations at South African PoEs is going to represent a major change in work habits and conditions for South African and its neighbouring countries' staff. It will first imply a new mind-set, with staff working side by side, and sometimes in an integrated manner. This will also lead to changes in some procedures and streamlined activities, which will be centred on the objectives rather than the institution. There will be a shift to minimal intervention when there are no grounds to suspect any fraudulent activity.

The emphasis at the OSBP will be on providing good conditions of control while offering greater facilitation to both travellers and commercial operations. Methods of work will change, facilities will need to be improved, and new equipment will be needed. This should be accompanied by a change management strategy, aimed at both officials and users (including clearing agents/brokers).

9.7 High-level OSBP implementation plan

The following critical interventions will be undertaken over the short- to medium-term to give effect to the OSBP implementation plan:

Intervention	Deliverable	Time frames
1. OSBP policy	Final OSBP policy approved by Cabinet	March 2022
2. OSBP legislation	OSBP Act finalised & enacted	March 2024
3. OSBP bilateral agreements with affected neighbouring countries	Draft OSBP bilateral agreements to be finalised in consultation with South Africa's 5 neighbouring countries (Zimbabwe, Botswana, Mozambique, eSwatini & Lesotho)	Work in progress
4. Redevelopment of six priority land PoEs as OSBPs	Appoint the public-private partnership service providers Construction commences to redevelop the Beit Bridge, Lebombo, Maseru Bridge, Kopfontein, Oshoek & Ficksburg PoEs as OSBPs. Construction completed & the six priority land PoEs are operational as OSBPs.	April 2022 – December 2025

NATIONAL TREASURY

NO. 1427 **31 DECEMBER 2020**

AMENDMENTS TO REGULATIONS IN TERMS OF BANKS ACT, 1990

The Minister of Finance has, in terms of section 90 of the Banks Act, 1990 (Act No. 94 of 1990), made amendments to the Regulations relating to Banks which were published in Government Notice No. R. 1029 of 12 December 2012, Government Notice No. R. 261 of 27 March 2015, Government Notice No. R. 309 of 10 April 2015, General Notice No. R. 297 of 20 May 2016 and Notice No. 724 of 18 December 2020, as set out in the Schedule.

SCHEDULE

Definitions

1. In this Schedule, "the Regulations" means the Regulations published under Government Notice No. R. 1029, in *Government Gazette* No. 35950 on 12 December 2012, as amended by-

   (a) Government Notice No. 261, published in *Government Gazette* No. 38616 of 27 March 2015;

   (b) Government Notice No. 309, published in *Government Gazette* No. 38682 of 10 April 2015;

   (c) Government Notice No. 297, published in *Government Gazette* No. 40002 of 20 May 2016; and

   (d) Notice No. 724, published in *Government Gazette* No. 44003 of 18 December 2020.

Substitution of form BA 200

2. The form set out in Annexure A to this notice is hereby substituted for form BA 200 immediately preceding regulation 23 of the Regulations.

Amendment of regulation 23 of the Regulations

3. Regulation 23 of the Regulations is hereby amended-

   (a) by the addition to the proviso to subregulation (3) of the following paragraph:

   "(iii) irrespective of whether the bank adopts the standardised approach or IRB approach for the measurement of the bank's exposure to credit risk, the bank shall apply the relevant requirements specified in regulation 31 of these Regulations in respect of the bank's equity investments in all types of funds that are held in the bank's banking book, including any off-balance sheet exposure, such as unfunded commitments to subscribe to a fund's future capital calls, provided that the said requirements specified in regulation 31 of these Regulations shall not apply to any exposure, including any underlying exposure held by a fund, that is required to be deducted from the bank's capital and reserve funds in accordance with the relevant requirements specified in regulation 38(5) of these Regulations.";

   (b) by the substitution in subregulation (6) for paragraph (g) of the following paragraph:

   "(g) In the case of off-balance-sheet exposure, other than-

   (i) unsettled securities;

   (ii) derivative contracts subject to counterparty credit risk as envisaged in subregulations (15) to (19);

   (iii) posted collateral that is subject to the relevant requirements specified in subregulation (18) relating to the standardised approach for counterparty credit risk or in subregulation (19) relating to the internal model method for counterparty credit risk; or

   (iv) securitisation or resecuritisation exposure as envisaged in paragraph (h) below,

   the bank shall convert the off-balance-sheet exposure to a credit equivalent amount by multiplying the said exposure with the relevant credit-conversion factor specified in table 2 below:";

   (c) by the insertion of the following two entries in column 2 of table 7 in subregulation (6)(j) in respect of transactions with specified counterparties that are assigned a risk weight of 0%, immediately after the entry that reads "World Bank Group, including the International Bank for Reconstruction and Development (IBRD) and the International Finance Corporation (IFC)":

   "Multilateral Investment Guarantee Agency (MIGA)
   International Development Association (IDA)";

   (d) by the insertion of the following two entries in column 2 of table 7 in subregulation (6)(j) in respect of transactions with specified counterparties that are assigned a risk weight of 0%, immediately after the entry that reads "Council of Europe Development Bank (CEDB)" of the following entries:

   "International Finance Facility for Immunization (IFFIm)
   Asian Infrastructure Investment Bank (AIIB)";

   (e) by the substitution in Table 7 in subregulation (6)(j) for the entire entry relating to assets to be risk weighted at

150%, of the following entry:

"Risk weight	Transactions with the following counterparties, including assets
150% or higher[1]	**Assets** Such assets as may be specified in writing by the Authority

1. As may be specified in writing by the Authority.";

(f) by the substitution in subregulation (9)(b)(viii)(A) for the words preceding subitem (i) of the following words:

"(A) shall in the case of a collateralised transaction calculate its adjusted exposure through the application of the formula specified below, which formula is designed to take into account the effect of the collateral and any volatility in the amount relating to the exposure or collateral. The formula is expressed as:";

(g) by the deletion in subregulation (9)(b)(viii) of item (B).

(h) by the substitution in subregulation (11)(m)(ii) for item (A) of the following item:

"(A) the potential future exposure arising from an interest-rate contract or currency swap contract, calculated in accordance with the relevant requirements related to the standardised approach specified in subregulation (18);";

(i) by the substitution for subregulation (15) of the following subregulation:

"(15) *Counterparty credit risk exposure and matters related thereto*

(a) Subject to the provisions of paragraph (b) and subregulation (16), for the measurement of a bank's exposure amount or EAD, risk-weighted exposure and related required amount of capital and reserve funds in respect of instruments, contracts or transactions that expose the reporting bank to counterparty credit risk, the bank may-

(i) at the discretion of the bank, use the standardised approach specified in subregulation (18) below, which standardised approach shall be available only for the measurement of the reporting bank's exposure to counterparty credit risk arising from OTC derivative instruments, exchange-traded derivative instruments and long settlement transactions, irrespective of whether the said instruments, transactions, contracts or agreements are recorded in the reporting bank's banking book or trading book, provided that-

(A) the bank's exposure to credit risk arising from securities financing transactions shall be calculated, among other things, in accordance with the relevant requirements specified in subregulations (8) and (9) of this regulation 23;

(B) when the standardised approach for the measurement of the bank's exposure to counterparty credit risk, in the Authority's discretion, does not sufficiently capture the risk inherent in the bank's relevant transactions, the Authority may require the bank to apply the standardised approach on a transaction-by-transaction basis, that is, without recognising any form or effect of netting;

(ii) subject to the prior written approval of and such further conditions as may be specified in writing by the Authority, in addition to the requirements specified in subregulation (19) below, use the internal model method specified in the said subregulation (19), provided that-

(A) a bank that obtained the approval of the Authority to adopt the internal model method shall only under exceptional circumstances or in respect of immaterial exposures be allowed to revert to the standardised approach for all or part of its exposure, provided that the bank shall in all cases demonstrate to the satisfaction of the Authority that the said reversion to the less sophisticated method does not lead to arbitrage in respect of the bank's required amount of capital and reserve funds;

(B) the internal model method may be applied by a bank that adopted the standardised approach or the IRB approach for the measurement of the bank's other exposures to credit risk;

(C) the internal model method shall be applied to all relevant exposures in a particular category of exposures that are subject to counterparty credit risk, except exposures that arise from long settlement transactions;

(D) the internal model method may be applied to measure the bank's exposure or

EAD amount relating to-

(i) only OTC derivative instruments;

(ii) only securities financing transactions; or

(iii) OTC derivative instruments and securities financing transactions,

irrespective of whether the said transactions, contracts or agreements are recorded in the reporting bank's banking book or trading book.

(iii) subject to the prior written approval of and such conditions as may be specified in writing by the Authority, use a combination of the aforementioned methods, provided that-

(A) the said approval of the Authority shall be granted only in exceptional cases and only during the initial implementation period of the internal model method;

(B) a bank that wishes to apply such a combination of methods shall together with its application to obtain the approval of the Authority to adopt the internal model method submit a plan to include all material counterparty exposures relating to a particular category of instruments or transactions in the said internal model method;

(C) in respect of all OTC derivative transactions and all long settlement transactions in respect of which the reporting bank has not obtained approval from the Authority to use the internal model method, the bank shall apply the standardised approach for counterparty credit risk.

(b) Irrespective of the method adopted by the reporting bank for the measurement of-

(i) the bank's exposure to counterparty credit risk, when the bank purchases credit derivative protection against a banking book exposure or against an exposure to counterparty credit risk, the bank shall in respect of the hedged exposure calculate its required amount of capital and reserve funds in accordance with the relevant requirements relating to credit derivative instruments specified in subregulations (9)(d), (12)(e), (12)(g), (14)(d) and (14)(f), that is, in accordance with the relevant substitution or double default requirements;

(ii) the bank's exposure to counterparty credit risk arising from OTC derivative instruments or securities financing transactions, the bank may adopt either of the methods envisaged in paragraph (a) above for the measurement of the bank's exposure or EAD arising from long settlement transactions, provided that-

(A) the bank shall continuously comply with the relevant requirements specified in these Regulations and such further requirements specified in writing by the Authority in respect of the selected method;

(B) notwithstanding the materiality of a long settlement transaction or position, in order to calculate the bank's required amount of capital and reserve funds relating to the said long settlement transaction or position, a bank that obtained the approval of the Authority to adopt the IRB approach for the measurement of the bank's exposure to credit risk may apply the risk weights specified in the standardised approach, in subregulation (8);

(iii) the bank's exposure to counterparty credit risk, the exposure amount or EAD relating to a particular counterparty shall be equal to the sum of the relevant exposure amounts or EADs calculated in respect of each relevant netting set relating to the said counterparty, provided that-

(A) for purposes of calculating the relevant amount of required capital and reserve funds for default risk in terms of the relevant requirements specified in this subregulation (15) read with the relevant requirements specified in subregulations (16) to (19), the relevant outstanding exposure or EAD amount shall be net of any incurred credit valuation adjustment (CVA) losses;

(B) unless specifically otherwise provided in this subregulation (15) read with the relevant requirements specified in subregulations (16) to (19), the relevant outstanding exposure or EAD amount for a given OTC derivative counterparty shall be the higher of-

(i) zero; or

(ii) the difference between the sum of all relevant exposure amounts or EADs across all relevant netting sets with the counterparty and the credit valuation adjustment (CVA) for that counterparty which has already been recognised by the bank as an incurred write-down or incurred CVA loss, which CVA loss shall be calculated without taking into account any offsetting debit valuation adjustments related to changes in the fair value of liabilities that are due to a change in the bank's own credit risk which have been deducted from capital, that is-

(aa) the incurred CVA loss deduced from the exposure to determine the outstanding exposure or EAD shall be the CVA loss gross of all relevant debit value adjustments related to changes in the fair value of liabilities that are due to a change in the bank's own credit risk which have been separately deducted from capital;

(bb) to the extent that the aforesaid debit value adjustments have not been separately deducted from the bank's capital, the incurred CVA loss used to determine the outstanding exposure or EAD shall be net of such debit value adjustments;

(C) the aforesaid reduction of exposure or EAD by incurred CVA losses shall not apply in the calculation of the relevant amount of required capital and reserve funds for CVA risk;

(iv) the bank's exposure to counterparty credit risk, a bank shall, in addition to any capital requirement for default risk related to counterparty credit risk, determine the relevant amount of required capital and reserve funds to cover risk related to mark-to-market losses on the bank's expected exposure to counterparty risk, which losses shall for purposes of these Regulations be referred to as CVA risk or CVA losses in respect of OTC derivatives, provided that-

(A) a bank, other than a bank that obtained the approval of the Authority for the use of the internal model method for the measurement of the bank's exposure to counterparty credit risk and the internal models approach for the measurement of specific risk as part of a bank's exposure to market risk, shall calculate-

(i) the relevant required amount of capital for default risk in accordance with the relevant requirements and formulae specified in this subregulation (15) read with the relevant requirements specified in subregulations (16) to (18);

(ii) the relevant additional required amount of capital for CVA risk in accordance with the relevant requirements and formula specified in paragraph (c) below;

(B) a bank that obtained the approval of the Authority for the use of the internal model method for the measurement of the bank's exposure to counterparty credit risk and the internal models approach for the measurement of specific risk as part of a bank's exposure to market risk, shall calculate the relevant additional required amount of capital for CVA risk in accordance with the relevant requirements and formula specified in subregulation (19)(h)(i) below, which approach shall be regarded as the advanced approach for the calculation of the relevant required amount of capital and reserve funds for CVA risk, capturing both general and specific credit spread risk, including stressed value-at-risk (VaR) but not incremental risk, and which formula shall form the basis of all relevant inputs into the bank's approved VaR model for bonds, that is, when the bank's approved VaR model is based on full repricing, the bank shall use the formula specified in subregulation (19)(h)(i) for its relevant calculations, provided that-

(i) all relevant VaR amounts shall be calculated in accordance with the relevant quantitative requirements specified in regulation 28(8) of these Regulations and shall be the sum of the non-stressed VaR component and the stressed VaR component, provided that when calculating-

(aa) the non-stressed VaR component, the bank shall use current parameter calibrations for expected exposure;

(bb) the stressed VaR component, the bank shall use future counterparty expected exposure (EE) profiles in accordance with the stressed exposure parameter calibrations specified in these Regulations, including the relevant requirements specified in

regulation 39(12) of these Regulations, provided that the period of stress for the credit spread parameters shall be the most severe one-year stress period contained within the three-year stress period used for the bank's exposure parameters,

Provided that the three-times multiplier inherent in the calculation of VaR and stressed VaR shall also apply in respect of the aforesaid calculations;

(ii) when the bank's approved VaR model is based on credit spread sensitivities for specific tenors, the bank shall base each relevant credit spread sensitivity on the formula specified in subregulation (19)(h)(ii)(A);

(iii) when the bank's approved VaR model uses credit spread sensitivities to parallel shifts in credit spreads, which shall for purposes of these Regulations be referred to as regulatory CS01, the bank shall use the formula specified in subregulation (19)(h)(ii)(B);

(iv) when the bank's approved VaR model uses second-order sensitivities to shifts in credit spreads, that is, spread gamma, the gammas shall be calculated based on the formula specified in subregulation (19)(h)(i);

(v) a bank that obtained the approval of the Authority for the use of the internal model method for the majority of its business, but the bank uses the Standardised Approach for counterparty credit risk for certain smaller portfolios, and the bank also obtained the approval of the Authority for the use of the internal models approach for the measurement of specific risk as part of a bank's exposure to market risk, shall include these non-internal-model-method netting sets into the CVA risk capital requirements in accordance with the relevant requirements specified in subregulation (19)(h)(i), provided that-

(aa) the Authority may instruct the bank in writing to use the method envisaged in paragraph (c) below for the relevant portfolios specified in writing by the Authority;

(bb) any relevant non-internal-model-method netting set shall be included into the advanced CVA risk capital requirement assuming a constant EE profile, where EE shall be set equal to the EAD as calculated in terms of the Standardised Approach for counterparty credit risk for a maturity equal to the maximum of-

(i) half of the longest maturity occurring in the netting set; and

(ii) the notional weighted average maturity of all relevant transactions in the netting set,

(cc) when a bank's internal model does not produce an expected exposure profile, the bank shall in the calculation of the relevant required amount apply the same approach as set out in sub-item (bb) above;

(vi) when the bank's approved market risk VaR model does not appropriately reflect the risk of credit spread changes, because the bank's VaR model, for example, does not appropriately reflect the specific risk of debt instruments issued by a particular counterparty, the bank shall not use the advanced approach for CVA envisaged in subregulation (19)(h)(i) for those relevant exposures, and instead the bank shall determine the required amount of capital for CVA risk through the application of the standardised method specified in paragraph (c) below, that is, the bank shall include in its advanced approach calculations only those exposures to counterparties for which the bank obtained the approval of the Authority to apply its internal model in respect of specific risk for the relevant exposures arising from debt instruments;

(vii) the additional required amount of capital for CVA risk shall be a standalone market risk requirement, calculated on the set of CVAs envisaged in this item (B) read with the relevant requirements specified in subregulation (19)(h)(i), for all the relevant collateralised and uncollateralised OTC derivative counterparties, together with eligible CVA

hedges, provided that, unless expressly otherwise provided in these Regulations, within the standalone required amount of capital for CVA risk, the bank shall not apply any offset against any other instrument on the bank's balance sheet;

(C) only hedges used by the bank to mitigate its exposure to CVA risk, and managed as such by the bank, shall be eligible for inclusion in the calculation of the bank's relevant required amount of capital and reserve funds for CVA risk, irrespective of whether the relevant required amount is calculated in terms of the standardised or VaR approach, provided that-

(i) the only hedges eligible for inclusion in the calculation of the bank's required amount of capital and reserve funds for CVA risk in terms of the standardised or VaR approach shall be single-name credit default swaps (CDSs), single-name contingent CDSs, other equivalent hedging instruments referencing the counterparty directly, and index CDSs, that is, counterparty risk hedges other than the instruments specified above shall be excluded from the calculation of the bank's relevant required amount of capital and reserve funds for CVA risk;

(ii) in the case of index CDSs-

(aa) the basis between any individual counterparty spread and the spreads of index CDS hedges shall in all relevant cases be reflected in the bank's VaR amount, even when a proxy is used for the spread of a counterparty, since idiosyncratic basis still needs to be reflected in such situations, provided that for all counterparties with no available spread, the bank shall use reasonable basis time series out of a representative bucket of similar names for which a spread is available;

(bb) when the envisaged basis is not reflected to the satisfaction of the Authority, the bank shall include in its relevant VaR amount only 50 per cent of the notional amount of the index hedge;

(iii) no tranched or nth-to-default CDS shall constitute an eligible CVA hedge;

(iv) any eligible hedge included in the relevant required amount of capital and reserve funds for CVA risk shall be removed from the bank's relevant calculation of required capital and reserve funds for market risk;

(v) when a CDS referencing an issuer is in the bank's inventory, and that issuer also happens to be an OTC counterparty but the CDS is not managed by the bank as a hedge of CVA risk, that CDS shall not be eligible to offset the CVA within the bank's relevant standalone VaR calculation of the required amount of capital and reserve funds for CVA risk;

(D) the bank shall exclude from the aforesaid additional required amount of capital and reserve funds for CVA risk-

(i) all relevant transactions with intragroup banks or other formally regulated intragroup financial entities that are subject to capital requirements similar or equivalent to these Regulations, which banks or entities are included in the consolidated amounts calculated in accordance with the relevant requirements specified in these Regulations in respect of consolidated supervision, provided that the Authority may in writing instruct a bank to include in its relevant calculations for CVA risk all such transactions with intragroup banks or other formally regulated intragroup financial entities as may be specified in writing by the Authority;

(ii) transactions with a central counterparty (CCP); and

(iii) securities financing transactions (SFT), provided that when SFT exposures are deemed by the Authority to be material, the Authority may in writing instruct a bank to include in its relevant calculations CVA loss exposures arising from SFT transactions;

(E) the bank shall calculate the relevant aggregate amount of required capital and reserve funds for counterparty credit risk and credit valuation adjustments in accordance with the relevant requirements specified in paragraph (d) below;

(v) the bank's exposure to counterparty credit risk arising from OTC derivative instruments or securities financing transactions, the bank shall calculate its relevant required amount of capital and reserve funds relating to any delivery-versus-payment transaction and any non-delivery-versus-payment or free-delivery transaction in accordance with the relevant requirements specified in subregulation (20) below;

(vi) the bank's exposure to counterparty credit risk, unless specifically otherwise provided in these Regulations, the bank may in respect of its exposure to counterparty credit risk apply an exposure value or EAD equal to zero-

(A) when the said exposure to counterparty credit risk relates to protection provided by the reporting bank in the form of a credit-default swap contract held in the bank's banking book, provided that the said contract-

(i) shall be treated in a manner similar to a guarantee provided by the reporting bank and in accordance with the relevant requirements specified in subregulations (9)(d), (12)(e) or (14)(d), as the case may be;

(ii) shall be subject to required capital and reserve funds in respect of the contract's full notional amount;

(B) when the said exposure to counterparty credit risk relates to purchased credit derivative protection and the reporting bank calculates its required amount of capital and reserve funds in respect of the hedged exposure in accordance with the relevant requirements specified in subparagraph (i) above;

(vii) the bank's exposure to counterparty credit risk, the bank shall comply with the relevant requirements specified in subregulation (17) below related to margin requirements for non-centrally cleared derivative instruments.

(c) Matters related to minimum required capital and reserve funds for CVA risk, calculated in terms of the standardised approach

(i) A bank, other than a bank that obtained the approval of the Authority for the use of the internal model method for the measurement of the bank's exposure to counterparty credit risk and the internal models approach for the measurement of specific risk as part of the bank's exposure to market risk, shall calculate the relevant additional required amount of capital and reserve funds on a portfolio basis, in accordance with the formula specified below:

$$K = 2.33 * \sqrt{h} * \sqrt{(A - B)^2 + C}$$

where:

$$A = \sum_i 0.5 * w_i * (M_i * EAD_i^{total} - M_i^{hedge} B_i)$$

$$B = \sum_{ind} w_{ind} * M_{ind} * B_{ind}$$

$$C = \sum_i 0.75 * w_i^2 * (M_i * EAD_i^{total} - M_i^{hedge} B_i)^2$$

h is the one-year risk horizon, in units of a year, h = 1.

$\mathbf{w_i}$ is the weight applicable to counterparty 'i', provided that-

(i) based on its external rating, counterparty 'i' shall be mapped to one of the seven weights specified in table 16 below:

Table 16

Rating[1]	Weight w_i
AAA	0.7%
AA	0.7%
A	0.8%
BBB	1.0%

BB	2.0%
B	3.0%
CCC	10.0%

1. **The notations used in this table relate to the ratings used by a particular credit assessment institution. The use of the rating scale of a particular credit assessment institution does not mean that any preference is given to a particular credit assessment institution. The assessments/ rating scales of other external credit assessment institutions recognised as eligible institutions in South Africa, may have been used instead.**

(ii) subject to the prior written approval of and such conditions as may be specified in writing by the Authority, when a counterparty does not have an external rating, the bank shall map the relevant internal rating of the counterparty to one of the relevant external ratings specified above

EAD_i^{total} is the exposure at default of counterparty 'i', aggregated across all relevant netting sets, including the effect of any relevant collateral in accordance with the relevant requirements specified in these Regulations for the Standardised Approach for counterparty credit risk or the Internal Model Method, provided that in the case of-

(i) a bank other than a bank that obtained the approval of the Authority to adopt the Internal Model Method for the measurement of the bank's exposure to counterparty risk, the bank shall apply the following discounting factor to the exposure:

$(1 - \exp(-0.05*M_i))/(0.05*M_i)$;

(ii) a bank that obtained the approval of the Authority to adopt the Internal Model Method for the measurement of the bank's exposure to counterparty risk, the relevant discount factor is already included in M_i, and no further discount shall be applied

B_i is the notional amount of purchased single name CDS hedges, which notional amounts shall be aggregated in the case of more than one position referencing counterparty 'i', and used to hedge the bank's exposure to CVA risk, provided that the bank shall apply the following discounting factor to the relevant notional amount:

$(1 - \exp(-0.05*M_i^{hedge}))/(0.05* M_i^{hedge})$

B_{ind} is the full notional amount of one or more index CDS of purchased protection, used to hedge the bank's exposure to CVA risk, provided that the bank shall apply the following discounting factor to the relevant notional amount:

$(1 - \exp(-0.05*M_{ind}))/(0.05* M_{ind})$

w_{ind} is the relevant weight applicable to index hedges, provided that the bank shall map indices to one of the seven weights (w_i) specified in table 16 above, based on the average spread of index 'ind'

M_i is the effective maturity of the relevant transactions with counterparty 'i', provided that-

(i) in the case of a bank other than a bank that obtained the approval of the Authority to adopt the Internal Model Method for the measurement of the bank's exposure to counterparty risk, M_i shall be the notional weighted average maturity as envisaged in regulation 23(13)(d)(ii)(B)(iii) of these Regulations, provided that M_i shall for purposes of this calculation not be capped at 5 years;

(ii) a bank that obtained the approval of the Authority to adopt the Internal Model Method for the measurement of the bank's exposure to counterparty risk shall calculate M_i in accordance with the relevant requirements specified in subregulation (19)(c)

$\mathbf{M_i^{hedge}}$ is the maturity of the hedge instrument with notional B_i, provided that in the case of several positions the bank shall aggregate the relevant quantities $M_i^{hedge} \cdot B_i$

$\mathbf{M_{ind}}$ is the maturity of the index hedge 'ind', provided that in the case of more than one index hedge position, it shall be the relevant notional weighted average maturity

Provided that, subject to the prior written approval of and such conditions as may be specified in writing by the Authority, when a counterparty is also a constituent of an index on which a CDS is used to hedge the bank's exposure to counterparty credit risk, the notional amount attributable to that relevant single name, as per its reference entity weight, may be subtracted from the relevant index CDS notional amount and treated as a single name hedge (Bi) of the individual counterparty with maturity based on the maturity of the index.

(d) Matters related to the calculation of the aggregate amount of required capital and reserve funds for counterparty credit risk and credit valuation adjustments

The aggregate amount of required capital and reserve funds related to a bank's exposure to counterparty credit risk and CVA risk, that is, default risk and the risk of mark-to-market losses in respect of specified exposures, shall in the case of-

(i) a bank that obtained the approval of the Authority for the use of the internal model method for the measurement of the bank's exposure to counterparty credit risk and the internal models approach for the measurement of specific risk as part of a bank's exposure to market risk, be equal to the sum of-

(A) the higher of the relevant required amount of capital and reserve funds for default risk calculated in terms of the internal model method based on-

(i) current parameter calibrations for EAD; or

(ii) stressed parameter calibrations for EAD,

Provided that when a bank that obtained the approval of the Authority for the use of the IRB approach can demonstrate to the satisfaction of the Authority that in its VaR calculations made in terms of the relevant requirements specified in subregulation (19)(h)(i), the relevant specific VaR model incorporates the effects of rating migrations, the bank shall calculate the risk weights applied to its relevant OTC derivative exposures with the full maturity adjustment as a function of PD and M set equal to 1, provided that when the bank is unable to demonstrate the aforesaid to the satisfaction of the Authority, the bank shall apply the full maturity adjustment function, through the application of the formula specified below:

$(1 - 1.5 \times b)^{-1} \times (1 + (M - 2.5) \times b)$

where:

M is the effective maturity; and

b is the maturity adjustment as a function of the PD,

as envisaged in subregulation (11)(d)(ii) read with the relevant requirements specified in subregulation (13)(d)(ii)(B)

and

(B) the relevant amount of required capital and reserve funds for CVA risk calculated in accordance with the relevant requirements specified in paragraph (b)(iv) above read with the relevant requirements specified in subregulation (19)(h) below;

(ii) a bank that obtained the approval of the Authority for the use of the internal model method for the measurement of the bank's exposure to counterparty credit risk, but not for the use of the internal models approach for the measurement of specific risk as part of a bank's exposure to market risk, be equal to the sum of-

(A) the higher of the relevant required amount of capital and reserve funds for default risk calculated in terms of the internal model method based on-

(i) current parameter calibrations for EAD; or

(ii) stressed parameter calibrations for EAD,

and

(B) the relevant amount of required capital and reserve funds for CVA risk calculated in accordance with the standardised approach specified in paragraph (c) above;

(iii) all banks other than the banks envisaged in subparagraphs (i) and (ii) above, be equal to the sum of-

(A) the relevant aggregate required amount for default risk calculated in accordance with the relevant requirements related to the said standardised approach for counterparty credit risk, for all relevant counterparties and instruments; and

(B) the relevant amount of required capital and reserve funds for CVA risk calculated in accordance with the standardised approach specified in paragraph (c) above.";

(j) by the substitution for subregulation (16) of the following subregulation:

"(16) *Exposure to central counterparties and matters related thereto*

(a) A bank shall calculate its relevant exposure to central counterparties arising from any OTC derivative instrument, exchange-traded derivative instrument, securities financing transaction or long settlement transaction, and the bank's related required amount of capital and reserve funds, in accordance with the relevant requirements specified in this subregulation (16), provided that-

(i) any relevant exposure arising from the settlement of cash transactions in respect of equities, fixed income, spot FX or spot commodities shall be calculated in accordance with the relevant requirements specified in subregulation (20) below, provided that in the case of any contributions to prepaid default funds covering settlement-risk-only products, the bank shall apply a risk weight of zero per cent;

(ii) when the clearing member-to-client leg of any relevant exchange-traded derivative transaction is conducted in terms of a bilateral agreement, both the client bank and the relevant clearing member shall calculate the relevant exposure amount and the required amount of capital and reserve funds in accordance with the relevant requirements related to an OTC derivative instrument, for which purposes the provisions of paragraph (b)(ii) below shall *mutatis mutandis* apply;

(iii) the provisions of subparagraph (ii) above shall apply *mutatis mutandis* to any relevant transaction between lower level clients and higher level clients in the case of any multi-level client structure;

(iv) the bank shall ensure that it continuously maintains sufficient capital and reserve funds for all relevant exposures related to counterparty credit risk, including in respect of any relevant exposure to a qualifying central counterparty, that is, the bank shall, for example, consider whether it needs to maintain capital in excess of the minimum required amount of capital and reserve funds specified in terms of the provisions of these Regulations when the bank's relevant transactions with a central counterparty give rise to more risky exposures than what is provided for or envisaged in these Regulations, or when the bank is uncertain whether or not the relevant counterparty is or may indeed be regarded as a qualifying central counterparty;

(v) when the bank acts as a clearing member, the bank shall continously assess through appropriate scenario analysis and stress testing whether the level of capital and reserve funds maintained against the bank's exposures to a central counterparty adequately addresses the risks inherent in the relevant transactions, which assessment shall, for example, include all relevant potential future exposure or contingent exposure resulting from future drawings on default fund commitments, and/or from secondary commitments to take over or replace offsetting transactions from clients of another clearing member when that clearing member defaults or becomes insolvent;

(vi) the bank shall on a regular basis monitor and report to its senior management and the appropriate committee of the bank's board of directors, all relevant exposures to central counterparties, including all relevant exposures arising from trading through a central counterparty and exposures arising from central counterparty membership obligations, such as default fund contributions;

(vii) when the bank clears derivative instruments, securities financing transactions or long settlement transactions through a qualifying central counterparty, the bank shall calculate

its relevant exposure amount and the related required amount of capital and reserve funds in accordance with the relevant requirements specified in paragraph (b) below, provided that-

(A) subject to the prior written approval of and such conditions as may be specified in writing by the Authority, when a central counterparty no longer complies with the relevant requirements related to a qualifying central counterparty, the bank may continue to treat all relevant transactions with that counterparty in accordance with the relevant requirements specified in paragraph (b) below, for a maximum period of up to three months following the date on which that counterparty no longer complies with the said requirements, whereafter the bank shall calculate its relevant exposure amount and the related required amount of capital and reserve funds in accordance with the relevant requirements specified in paragraph (c) below;

(B) when the sum of the bank's relevant capital requirements in respect of exposures to a qualifying central counterparty related to its relevant trade exposures and default fund contributions is higher than the total capital requirement that would apply to those same exposures if the central counterparty was a non-qualifying central counterparty, the bank shall maintain the latter required amount of capital and reserve funds in respect of its relevant exposures, that is, the total capital requirement in respect of all relevant exposures to a qualifying central counterparty shall not exceed the total capital requirement for the same exposures if the central counterparty was a non-qualifying central counterparty;

(viii) when the bank clears derivative instruments, securities financing transactions or long settlement transactions through a non-qualifying central counterparty, the bank shall calculate its relevant exposure amount and the related required amount of capital and reserve funds in accordance with the relevant requirements specified in paragraph (c) below.

(b) *Exposures to qualifying central counterparties*

(i) *Clearing member trade exposures to qualifying central counterparties*

Subject to the provisions of subparagraph (v) below, when a bank acts as a clearing member of a qualifying central counterparty for its own purposes, the bank shall in respect of all relevant OTC derivative transactions, exchange traded derivative transactions, securities financing transactions and long-settlement transactions apply a risk weight of 2 per cent to the bank's relevant trade exposure to the qualifying central counterparty, provided that-

(A) when the said bank acting as a clearing member offers clearing services to clients, the 2 per cent risk weight shall also apply to the clearing member's trade exposure to the qualifying central counterparty that arises when the clearing member is obligated to reimburse the client for any losses suffered due to changes in the value of its transactions in the event that the qualifying central counterparty defaults, provided that the bank shall determine the risk weight to be applied to any collateral posted by the bank to the relevant qualifying central counterparty in accordance with the relevant requirements specified in subparagraph (v) below;

(B) the bank shall calculate the relevant exposure amount for such trade exposure in accordance with the relevant requirements related to the standardised approach or the internal model method for exposure to counterparty credit risk, respectively specified in subregulations (18) and (19) below, as the case may be, read with the relevant requirements specified in subregulation (9) in respect of collateralised exposure, provided that-

(i) in all relevant cases, when the bank wishes to calculate the relevant exposure amount for any relevant trade exposure in accordance with the internal model method, the bank shall apply to the Authority to obtain the Authority's prior written approval to extend the scope of the internal model method to include centrally cleared products, that is, even when the bank obtained the prior written approval of the Authority to include non-centrally cleared products, the bank shall not extend the scope of the internal model method to include centrally cleared products without the explicit prior written approval of the Authority;

(ii) in the case of a bank that obtained the approval of the Authority to adopt the internal model method, the relevant specified 20-day floor for the margin period of risk, related to the number of transactions, shall not

apply, provided that the relevant netting set does not contain illiquid collateral or exotic trades, and there are no disputed trades;

(iii) in all relevant cases the bank shall apply a minimum margin period of risk of 10 days for the calculation of trade exposures to central counterparties in respect of OTC derivative transactions or instruments;

(iv) when a central counterparty retains variation margin against certain trades, such as, for example, when a central counterparty collects and holds variation margin against positions in exchange-traded or OTC forwards, and the member collateral is not protected against the insolvency of the central counterparty, the minimum time risk horizon applied to the bank's relevant trade exposures on those trades shall be the lesser of one year and the remaining maturity of the transaction, subject to a floor of 10 business days;

(C) when settlement is legally enforceable on a net basis in an event of default, regardless of whether the counterparty is insolvent or bankrupt, the bank may calculate the relevant total replacement cost of all contracts relevant to the trade exposure determination on a net replacement cost basis, provided that the relevant close-out netting sets-

(i) shall in the case of all relevant repo-style transactions comply with all the relevant requirements specified in subregulation (9)(b)(xvi);

(ii) shall in the case of all relevant transactions in derivative instruments comply with all the relevant requirements specified in subregulation (18);

shall in all relevant cases related to cross-product netting comply with all the relevant requirements specified in subregulation (19)(d):

Provided that when a bank is unable to demonstrate to the satisfaction of the Authority that all relevant netting agreements duly comply with the aforesaid requirements, the bank shall regard each relevant single transaction as a netting set of its own for purposes of calculating its relevant trade exposure amount.

(ii) *Clearing member trade exposures to clients*

Without derogating from the provisions of subparagraph (v) below, a bank that acts as a clearing member shall in all relevant cases calculate its relevant exposures, including any potential CVA risk exposure, to clients as bilateral trades, irrespective of whether the clearing member guarantees the trade or acts as an intermediary between the client and the relevant qualifying central counterparty, provided that-

(A) in order to recognise the shorter close-out period for cleared client transactions, a bank that acts as a clearing member and that adopted either the standardised approach or the internal model method for the measurement of the bank's exposure to counterparty credit risk may calculate its relevant exposure amount to clients and the related required amount of capital and reserve funds by applying a margin period of risk of no less than 5 days, provided that the bank shall also use the resultant reduced EAD amount for the calculation of any relevant capital requirement for CVA risk in terms of the standardised or advanced approach or method;

(B) when a bank that acts as a clearing member collects collateral from a client in respect of client cleared trades and that collateral is passed on to the relevant central counterparty, the bank may recognise that collateral for both the central counterparty clearing member leg and the clearing member-client leg of the relevant client cleared trade.

Therefore, the initial margin posted by clients to their clearing member mitigates the exposure the clearing member has against these clients. The same treatment shall apply in a similar manner to multi-level client structures, between a higher level client and a lower level client.

(iii) *Client trade exposures: clearing member acting as a financial intermediary*

When a bank is a client of a clearing member, and the bank enters into a transaction with the said clearing member acting as a financial intermediary, that is, the clearing member completes an offsetting transaction with a qualifying central counterparty, the bank's exposures to the clearing member may be calculated in accordance with the relevant

requirements specified in subparagraph (i) above, provided that-

(A) the relevant qualifying central counterparty shall identify the relevant offsetting transactions as client transactions and the qualifying central counterparty and/or the clearing member, as the case may be, shall hold collateral to support the relevant transactions, in a manner that prevents any losses to the client due to-

(i) the default or insolvency of the clearing member;

(ii) the default or insolvency of the clearing member's other clients; and

(iii) the joint default or insolvency of the clearing member and any of its other clients.

That is, upon the insolvency of the clearing member, there shall be no legal impediment, other than the need to obtain a court order to which the client is entitled, to the transfer of the collateral belonging to the clients of a defaulting clearing member to the qualifying central counterparty, to one or more other surviving clearing members or to the client or the client's nominee.

(B) the relevant bank or client shall have conducted a robust legal review, and shall undertake such further review(s) as may be necessary to ensure continued enforceability, and have a well-founded legally enforceable basis to conclude that, in the event of legal challenge, the relevant courts and administrative authorities would find that the aforesaid arrangements are legal, valid, binding and enforceable in terms of all the relevant laws of all the relevant jurisdictions;

(C) relevant laws, regulation, rules, contractual, or administrative arrangements shall provide that the offsetting transactions with the defaulted or insolvent clearing member are highly likely to continue to be indirectly transacted through the relevant qualifying central counterparty, or by the qualifying central counterparty, if the clearing member defaults or becomes insolvent, and in which case the client positions and collateral with the relevant qualifying central counterparty shall be transferred at market value, unless the client requests to close out the position at market value;

(D) when all the relevant conditions and requirements specified in the preceding items (A) to (C) of this subparagraph (iii) are met, except that the relevant client is not protected from losses in the case that the clearing member and another client of the clearing member jointly default or become jointly insolvent, a risk weight of 4 per cent shall apply in respect of the relevant client exposure to the clearing member, or to the relevant higher level client exposure in a multi-level client structure, respectively;

(E) when the bank is a client of the clearing member and the conditions and requirements envisaged in items (A) to (D) hereinbefore are not met, the bank shall calculate all relevant exposures and the related required amount of capital and reserve funds, including any relevant CVA risk exposure, to the relevant clearing member on a bilateral trade basis;

(F) when all the relevant conditions and requirements specified in the preceding items (A) to (C) of this subparagraph (iii) are met in respect of all the relevant client exposures of lower level clients to higher level clients in a multi-level client structure, that is, in respect of all the relevant client levels in-between, the provisions of subparagraph (i) above may be applied to the relevant exposures of all the said client levels in-between.

(iv) *Client trade exposures: clearing member guaranteeing performance*

When a bank that is a client of a clearing member enters into a transaction with a qualifying central counterparty, and the clearing member guarantees the bank's performance, the bank's exposures to the qualifying central counterparty may be calculated in accordance with the relevant requirements specified in subparagraph (i) above, provided that-

(A) the relevant qualifying central counterparty shall identify the relevant offsetting transactions as client transactions and the qualifying central counterparty and/or the clearing member, as the case may be, shall hold collateral to support the relevant transactions, in a manner that prevents any losses to the client due to-

(i) the default or insolvency of the clearing member;

(ii) the default or insolvency of the clearing member's other clients; and

(iii) the joint default or insolvency of the clearing member and any of its other clients.

That is, upon the insolvency of the clearing member, there shall be no legal impediment, other than the need to obtain a court order to which the client is entitled, to the transfer of the collateral belonging to the clients of a defaulting clearing member to the qualifying central counterparty, to one or more other surviving clearing members or to the client or the client's nominee.

(B) the relevant bank or client shall have conducted a robust legal review, and shall undertake such further review(s) as may be necessary to ensure continued enforceability, and have a well-founded legally enforceable basis to conclude that, in the event of legal challenge, the relevant courts and administrative authorities would find that the aforesaid arrangements are legal, valid, binding and enforceable in terms of all the relevant laws of all the relevant jurisdictions;

(C) relevant laws, regulation, rules, contractual, or administrative arrangements shall provide that the offsetting transactions with the defaulted or insolvent clearing member are highly likely to continue to be indirectly transacted through the relevant qualifying central counterparty, or by the qualifying central counterparty, if the clearing member defaults or becomes insolvent, and in which case the client positions and collateral with the relevant qualifying central counterparty shall be transferred at market value, unless the client requests to close out the position at market value;

(D) when all the relevant conditions and requirements specified in the preceding items (A) to (C) of this subparagraph (iv) are met, except that the relevant client is not protected from losses in the case that the clearing member and another client of the clearing member jointly default or become jointly insolvent, a risk weight of 4 per cent shall apply to the relevant client exposure to the clearing member, or to the relevant higher level client exposure in a multi-level client structure, respectively;

(E) when the bank is a client of the clearing member and the conditions and requirements envisaged in items (A) to (D) hereinbefore are not met, the bank shall calculate all relevant exposures and the related required amount of capital and reserve funds, including any relevant CVA risk exposure, to the relevant clearing member on a bilateral trade basis.

(v) *Matters related to posted collateral*

In all relevant cases, any asset or collateral posted or provided shall, from the perspective of the bank posting or providing such collateral, be assigned the relevant risk weight that otherwise applies to such asset or collateral in terms of the relevant provisions or requirements specified in these Regulations, regardless of the fact that such asset has been posted or provided as collateral, that is, all collateral posted shall be subject to the relevant requirements specified in these Regulations related to banking book or trading book positions, as the case may be, as if the collateral had not been posted to the relevant central counterparty, provided that-

(A) in addition, the said collateral shall be subject to the relevant requirements specified in these Regulations related to counterparty credit risk exposures, irrespective of whether such collateral is held in the bank's banking book or trading book;

(B) when an asset or collateral of a clearing member or client is posted with or provided to a qualifying central counterparty or a clearing member, and the asset or collateral so posted or provided is not held in a bankruptcy remote manner, the bank posting or providing such asset or collateral shall also recognise the related credit risk exposure, based upon the asset or collateral being exposed to a risk of loss that is based on the creditworthiness of the entity or person holding such asset or collateral, provided that-

(i) when the entity or person holding such asset or collateral is the qualifying central counterparty, a risk weight of 2 per cent shall apply to collateral included in the definition of trade exposure; and

(ii) the relevant risk weight of the qualifying central counterparty shall apply to assets or collateral posted or provided for any purpose other than the

situation provided for in the aforesaid sub-item (i) above;

(C) a bank that adopted-

(i) the standardised approach for the measurement of its exposure to counterparty credit risk shall account for collateral posted not held in a bankruptcy remote manner in the relevant NICA term, in accordance with the relevant requirements specified in subregulation (18) below;

(ii) the internal model method for the measurement of its exposure to counterparty credit risk shall apply the relevant specified alpha multiplier envisaged in subregulation (19) below to the relevant exposure related to the posted collateral;

(D) all relevant collateral posted or provided by a clearing member, including cash, securities, other pledged assets, and excess initial or variation margin, which is often being referred to as overcollateralisation, that is held by a custodian, and is bankruptcy remote from the relevant qualifying central counterparty, shall not be subject to a capital requirement for counterparty credit risk exposure to such bankruptcy remote custodian, that is, the related risk weight or EAD shall be equal to zero, provided that for purposes of this item (D), custodian includes a trustee, agent, pledgee, secured creditor or any other person that holds property in a manner that does not give such person a beneficial interest in such property and will not result in such property being subject to legally-enforceable claims by such person's creditors, or to a court-ordered stay of the return of such property, should such a person become insolvent or bankrupt;

(E) in relation to collateral that is posted by a client and held by a custodian, and is bankruptcy remote from the relevant qualifying central counterparty, the clearing member and other clients shall not be subject to a capital requirement for counterparty credit risk, provided that when the collateral is held at the qualifying central counterparty on a client's behalf and is not held on a bankruptcy remote basis-

(i) a risk weight of 2 per cent shall apply to that collateral only when all the relevant conditions and requirements envisaged in paragraphs (b)(iii)(A) to (b)(iii)(C) above are met;

(ii) a risk weight of 4 per cent shall apply to that collateral when the relevant conditions envisaged in paragraph (b)(iii)(D) apply;

(vi) *Matters related to default fund exposures*

When a default fund is shared between products or types of business with settlement risk only, such as, for example, equities and bonds, and products or types of business which give rise to counterparty credit risk, such as, for example, OTC derivative instruments, exchange-traded derivative instruments, securities financing transactions or long settlement transactions, the risk weight determined in accordance with the relevant formulae and methodology specified in subparagraph (vii) below shall be assigned to the relevant aggregate amount of all of the said default fund contributions, without any apportionment to the different classes or types of business or products, provided that-

(A) when the default fund contributions from clearing members are segregated by product types and are only accessible for specific product types, the relevant capital requirements for those default fund exposures shall be determined for each relevant product giving rise to counterparty credit risk, in accordance with the formulae and methodology specified in subparagraph (vii) below;

(B) when the relevant qualifying central counterparty's prefunded own resources are shared among product types, the qualifying central counterparty shall allocate those funds to each of the relevant calculations, in proportion to the respective product-specific exposure or EAD amount;

(C) when a bank acting as a clearing member is required to calculate a required amount of capital and reserve funds related to exposures arising from default fund contributions to a qualifying central counterparty, the bank shall calculate the said required amount of capital and reserve funds in accordance with the formulae and methodology set out in subparagraph (vii) below.

(vii) *Formulae and methodology to be applied in respect of default fund exposures*

(A) Based on the risk sensitive formulae specified in items (B) and (C) below, that consider-

(i) the size and quality of a qualifying central counterparty's financial resources;

(ii) the counterparty credit risk exposures of such qualifying central counterparty; and

(iii) the application of such financial resources via the qualifying central counterparty's loss bearing waterfall, in the case of one or more clearing member defaults,

a bank that acts as a clearing member shall apply the relevant specified risk weight for its default fund contributions, provided that, in this regard, the bank's risk sensitive capital requirement for its default fund contribution, denoted by K_{CMi}, shall be calculated in accordance with the formulae and methodology specified in items (B) and (C) below, which calculations-

(aa) may also be performed by a qualifying central counterparty, supervisor or any other person with access to the relevant required data;

(bb) shall be made only when the relevant conditions and requirements specified in item (D) below, are met.

(B) Any relevant person that wishes to calculate the relevant required amount of capital and reserve funds and the related risk weight envisaged in this subparagraph (vii) shall firstly calculate the hypothetical capital requirement of the qualifying central counterparty due to its counterparty credit risk exposures to all of its relevant clearing members and their clients, through the application of the formula specified below, provided that-

(i) the holding periods related to securities financing transactions specified in subregulation (9)(b)(xiv) and those for derivative instruments specified in subregulation (19)(e) shall apply even if more than 5000 trades are within one netting set, that is, the higher specified supervisory floor for more than 5000 trades shall not apply in this case;

(ii) the netting sets that apply to regulated clearing members shall be the same as those envisaged in paragraph (b)(i)(C) above, provided that, for all other clearing members, the netting rules specified by the relevant qualifying central counterparty based upon notification of each of its clearing members, or such requirements related to netting sets as may be specified in writing by the Authority, shall apply

$$K_{CCP} = \sum_{CM\,i} EAD_i \cdot RW \cdot capital\ ratio$$

where:

K_{CCP}	is the hypothetical capital requirement for a qualifying central counterparty, calculated for the sole purpose of determining the capitalisation of clearing member default fund contributions, that is, K_{CCP} does not represent the actual capital requirements for a qualifying central counterparty, which may be determined separately by the relevant qualifying central counterparty and/or its relevant supervisor
RW	is a minimum risk weight of 20 per cent, or such a higher risk weight as may be specified in writing by the Authority, for example, when the clearing members related to a qualifying central counterparty are not highly rated
Capital ratio	shall be 8 per cent
EAD_i	is the relevant exposure amount of the qualifying central counterparty to clearing member 'i', including both the clearing member's own transactions and client transactions guaranteed by the clearing member, and all relevant amounts

of collateral held by the central counterparty, including the clearing member's prefunded default fund contribution, against the relevant transactions, in respect of the valuation at the end of the relevant regulatory reporting date, before the margin called on the final margin call of that day is exchanged:

Provided that-

(i) when clearing members provide client clearing services, and client transactions and collateral are held in individual or omnibus separate sub-accounts to the clearing member's proprietary business, each such client sub-account shall be included in the sum separately, that is-

(aa) in order to ensure that client collateral cannot offset the central counterparty's exposures to clearing members' proprietary activity in the calculation of K_{CCP}, the member EAD in the aforesaid formula shall be the sum of the client sub-account EADs and any relevant house sub-account EAD;

(bb) when any sub-account contains both derivatives and securities financing transactions, the EAD of that sub-account shall be the sum of the derivative EAD and the securities financing transactions EAD;

(ii) when collateral is held against an account containing both securities financing transactions and derivative transactions, the prefunded initial margin provided by the member or client shall be allocated to the relevant securities financing transactions and derivatives exposures, in proportion to the respective product-specific EADs, calculated in accordance with the relevant requirements specified in subregulations (8) and (9) for securities financing transactions and the standardised approach for the measurement of the bank's exposure to counterparty credit risk specified in subregulation (18), without including the effect of any collateral, for derivative instruments;

(iii) when the default fund contributions of the member, denoted by DF_i in the relevant formulae, are not split with regard to client and house sub-accounts, the said contributions shall be allocated per sub-account according to the respective fraction the initial margin of that sub-account has in relation to the total initial margin posted by or for the account of the relevant clearing member;

(iv) in the case of derivative instruments-

(aa) EAD_i shall be calculated as the bilateral trade exposure the relevant central counterparty has against the relevant clearing member, calculated in accordance with the relevant requirements specified in subregulation (18) below, applying a margin period of risk of 10 days to calculate the central counterparty's potential future exposure to its clearing member;

(bb) all collateral held by the relevant central counterparty to which that central counterparty has a legally enforceable claim in the event of the default of the relevant member or client, including any relevant default fund contributions of that member, denoted by DF_i in the relevant formulae, shall

be used to offset the central counterparty's exposure to that member or client, through inclusion in the relevant PFE multiplier, as set out in subregulation (18) below;

(v) in the case of securities financing transactions, EAD shall be equal to-

$\max(EBRM_i - IM_i - DF_i; 0)$,

where:

$EBRM_i$ is the exposure value to clearing member 'i' before the application of any risk mitigation in terms of the relevant provisions of subregulation (9)(b), and where, for purposes of this calculation, variation margin that has been exchanged, before the margin called on the final margin call of that day, enters into the mark-to-market value of the relevant transactions

IM_i is the relevant initial margin collateral posted by the relevant clearing member with the qualifying central counterparty

DF_i is the relevant prefunded default fund contribution by the relevant clearing member that will be applied upon such clearing member's default, either along with or immediately following such member's initial margin, to reduce the qualifying central counterparty loss

Provided that any haircuts to be applied in respect of the relevant securities financing transactions shall be the relevant standardised haircuts specified in subregulation (9)(b)(xi).

Σ means the relevant sum in respect of all the relevant clearing member accounts

(C) Following the first-step calculation envisaged in item (B) above, the capital requirement for each relevant clearing member shall be calculated through the application of the formula specified below, which formula effectively imposes a floor of 2 per cent on the risk weight for the default fund exposure:

$$K_{CM_i} = \max\left\{ K_{CCP} \cdot \left(\frac{DF_i^{pref}}{DF_{CCP} + DF_{CM}^{pref}} \right); 8\% * 2\% * DF_i^{pref} \right\}$$

where:

K_{CMi} is the capital requirement on the default fund contribution of member i

DF_{CM}^{pref} is the total prefunded default fund contributions from clearing members

DF_{CCP} is the central counterparty's prefunded own resources, such as, for example, contributed capital and retained earnings, which are contributed to the default waterfall, where these rank junior to or *pari passu* with prefunded member contributions

DF_i^{pref} is the prefunded default fund contributions provided by clearing member i

(D) In all cases, any relevant central counterparty, bank, supervisor or other person with access to the relevant required data shall calculate K_{CCP}, DF_{CM}^{pref} and DF_{CCP}

in accordance with the relevant requirements specified hereinbefore, and shall make available sufficient information related to the said calculations-

(i) to allow the Authority or any relevant supervisor of the qualifying central counterparty to appropriately oversee the said calculations;

(ii) to permit each relevant clearing member to calculate its capital requirement for the default fund; and

(iii) for the relevant supervisor of such clearing member to review and confirm the required calculations,

provided that, as a minimum-

(aa) K_{CCP} shall be calculated on a quarterly basis, or on such a more frequent basis as may be specified in writing by the Authority;

(bb) whichever person makes the aforesaid calculations shall, whenever required or requested, make available to the relevant supervisor of any relevant bank clearing member sufficient aggregate information regarding the composition of the qualifying central counterparty's exposures to the clearing members, and information provided to the clearing member for the purposes of the calculation of K_{CCP}, DF_{CM}^{pref} and DF_{CCP};

(cc) the aforesaid relevant required information shall be made available to the relevant supervisor on a sufficiently frequent basis to allow the supervisor to duly monitor the risks incurred by the relevant clearing member(s);

(dd) K_{CCP} and K_{CMi} shall be recalculated at least quarterly, or whenever material changes occur in respect of, for example, the number or exposure of cleared transactions, or the financial resources of the relevant qualifying central counterparty.

(c) Exposures to non-qualifying central counterparties

(i) Trade exposures

Based on the relevant type or category of counterparty credit exposure, a bank shall apply the relevant requirements specified in these Regulations related to the standardised approach for credit risk in respect of the bank's trade exposure to a non-qualifying central counterparty to calculate the relevant required credit exposure amount and the related required amount of capital and reserve funds;

(ii) Default fund contributions

A bank shall apply a risk weight of 1250 per cent in respect of the bank's default fund contributions to a non-qualifying central counterparty, which default fund contributions shall for purposes of this paragraph (c) include both the funded and the unfunded contributions to be paid when required by the relevant central counterparty, provided that in respect of any liability for unfunded contributions, that is, any relevant unlimited binding commitment, the Authority shall specify in writing the relevant amount of unfunded commitment to which the bank shall apply the aforesaid risk weight of 1250 per cent.";

(k) by the substitution for subregulation (17) of the following subregulation:

"(17) *Margin requirements for non-centrally cleared derivative instruments and matters related thereto*

In order to mitigate the potential systemic risk that may arise from and to promote effective and sound risk management in respect of a bank's transactions in non-standardised non-centrally cleared derivative instruments a bank shall-

(a) calculate and exchange-

(i) initial margin;

and

(ii) variation margin,

in accordance with such requirements as may be specified from time to time in a Joint Standard or Prudential Standard issued in terms of the Financial Sector Regulation Act, 2017;

(b) have in place robust processes, procedures and board-approved policies in respect of the bank's derivatives transactions that are not cleared through a central counterparty.";

(l) by the substitution for subregulation (18) of the following subregulation:

"(18) *Calculation of counterparty credit exposure or EAD in terms of the standardised approach*

(a) *Matters relating to the exposure amount or EAD*

A bank that adopted the standardised approach for the measurement of the bank's exposure to counterparty credit risk-

(i) shall calculate its relevant exposure to counterparty credit risk or the relevant EAD amount in respect of each relevant netting set through the application of the formula specified below:

The exposure amount or EAD shall be equal to-

alpha * (RC + PFE)

where:

alpha is equal to 1.4

RC is the relevant replacement cost, calculated in accordance with the relevant requirements specified in subparagraph (ii) below

PFE is the relevant potential future exposure amount, calculated in accordance with the relevant requirements specified in subparagraph (iii) below

(ii) shall calculate the relevant replacement cost component of the formula specified in subparagraph (i) above in accordance with the requirements specified in this subparagraph (ii), provided that-

(A) the bank shall calculate the replacement cost amount at the level of each relevant netting set, provided that-

(i) when the bank owes the relevant counterparty money, the bank has no replacement cost, since the bank will be able to instantly replace its trades and sell collateral at current market prices without any loss or cost to the bank in the case that the counterparty defaults;

(ii) the relevant replacement cost shall in no case be less than zero;

(iii) when the bank enters into multiple margin agreements that apply to a single netting set, the bank shall divide the netting set into sub-netting sets that align with their respective margin agreement;

(iv) when the bank holds excess collateral, even in the absence of a margin agreement, or the bank has out-of-the-money trades that can further protect the bank from an increase in its relevant counterparty exposure, the bank may reduce the relevant potential future exposure add-on amount with such over-collateralisation or negative mark-to market value, but the said over-collateralisation or negative mark-to-market value shall in no case affect the replacement cost envisaged in this subparagraph (ii);

(B) the bank shall treat any bilateral transaction with a one-way margining agreement in favour of the bank's counterparty, that is, when the bank is required to post, but does not collect, collateral, as an unmargined transaction;

(C) the bank shall only apply any form of netting between amounts in the calculation of the relevant replacement cost component when all the conditions specified in paragraph (b) below are met;

(D) for purposes of these Regulations, in the case of margined trades or transactions-

(i) the relevant replacement cost shall be the largest exposure amount to the relevant counterparty without triggering a call for variation margin, taking

into account the relevant mechanics of collateral exchange in the bank's relevant margining agreement, including, for example, "Threshold", "Minimum Transfer Amount" and "Independent Amount" arrangements, which may be factored into a call for variation margin;

(ii) the independent collateral amount, denoted by ICA-

(aa) means-

(i) collateral other than variation margin posted by the relevant counterparty, which the bank may seize when the counterparty defaults, the amount of which does not change in response to the value of the transactions it secures; and/or

(ii) the Independent Amount, denoted by IA, parameter, as often defined in standardised documentation;

(bb) may change in response to factors such as the value of the collateral or a change in the number of transactions in the netting set;

(iii) the net independent collateral amount, denoted by NICA-

(aa) means-

(i) the relevant aggregate amount of segregated or unsegregated collateral posted by the relevant counterparty, less the aggregate amount of unsegregated collateral posted by the bank; or

(ii) the amount of collateral that the bank may use to offset its exposure when the relevant counterparty defaults;

(bb) shall not include collateral that the bank has posted to a segregated, bankruptcy remote account, which presumably would be returned upon the bankruptcy of the counterparty;

(cc) takes into account the differential of the IA required for the bank minus the IA required for the relevant counterparty;

(iv) the relevant replacement cost may be stated mathematically as:

RC = max{V *minus* C; TH *plus* MTA *minus* NICA; 0}

where:

V is the value of the relevant derivative transactions in the netting set

C is the haircut value of the net collateral held, which shall be calculated in accordance with the NICA methodology specified hereinbefore, provided that for purposes of this calculation the value of non-cash collateral posted by the bank to its counterparty shall be increased by, and the value of the non-cash collateral received by the bank from its counterparty shall be decreased by, the relevant haircuts specified in these Regulations from time to time in respect of repo-style transactions

TH is the positive threshold before the counterparty is required to send the bank collateral

MTA is the minimum transfer amount applicable to the relevant counterparty

TH + MTA – NICA:
is the largest exposure amount to the relevant counterparty without triggering a call for variation margin, and it contains levels of collateral that have to be maintained at all times.

For example, without initial margin or IA, the largest exposure that would not trigger a variation margin call is the threshold plus any minimum transfer amount.

In the formulation, NICA is subtracted from TH + MTA in order to fully reflect both the actual level of exposure that would not trigger a margin call and the effect of collateral held and/or posted by the bank.

The aforesaid calculation is subject to a floor amount of zero, recognising that the bank may hold NICA in excess of TH + MTA, which could otherwise result in a negative replacement cost;

(v) the purpose of-

(aa) the calculation of the relevant replacement cost is to capture the probable loss that is likely to occur if the counterparty defaults, assuming that the closeout and replacement of transactions occur instantaneously;

(bb) the calculation of the relevant potential future exposure add-on in terms of the requirements specified in subparagraph (iii) below is to capture the potential change in the value of the trades during the so-called margin period of risk, that is, the period between the last exchange of collateral before default and the replacement of the trades in the market; and

(cc) the haircut applicable to non-cash collateral is to reflect the potential change in the value of the collateral during the relevant margin period of risk;

(E) for purposes of these Regulations, in the case of unmargined transactions, that is, when no variation margin is exchanged, although collateral other than variation margin may be exchanged-

(i) the relevant replacement cost shall be the greater of:

(aa) the current market value of the relevant derivative contracts less the net haircut collateral held by the bank, if any; or

(bb) zero,

which may be stated mathematically as:

replacement cost (RC) = max{V – C; 0}

where:

V is the value of the relevant derivative transactions in the netting set

C is the haircut value of the net collateral held, which shall be calculated in accordance with the NICA methodology specified in subparagraph (ii)(D)(iii) above, provided that for purposes of this calculation the value of non-cash collateral posted by the bank to its counterparty shall be increased by, and the value of the non-cash collateral received by the bank from its counterparty shall be decreased by, the relevant haircuts specified in these Regulations from time to time in respect of repo-style transactions

(ii) the purpose of-

(aa) the calculation of the relevant replacement cost is to capture the probable loss that is likely to occur if the counterparty defaults and all relevant transactions are closed out immediately;

(bb) the calculation of the relevant potential future exposure add-on in terms of the requirements specified in subparagraph (iii) below is to capture the potential conservative increase in exposure over a one-year time horizon from the relevant reporting or calculation

date; and

(cc) the haircut applicable to non-cash collateral is to reflect the potential change in the value of the collateral during the said one-year time period;

(F) when a single margin agreement applies to several netting sets, and, as such, it is problematic to allocate any common collateral to individual netting sets, the bank shall calculate the relevant replacement cost as the sum of two components, as follows:

(i) the unmargined current exposure of the bank to the relevant counterparty, aggregated across all the relevant netting sets within the margin agreement, reduced by the positive current net collateral, that is, collateral is subtracted only when the bank is a net holder of collateral, provided that the said net collateral amount available to the bank shall include both VM and NICA;

(ii) the current net posted collateral, if any, reduced by the unmargined current exposure of the relevant counterparty to the bank, aggregated across all the relevant netting sets within the margin agreement, which component can be non-zero only when the bank is a net poster of collateral;

(iii) RC for the entire margin agreement is therefore calculated as follows:

$$RC_{MA} = \max\left\{\sum_{NS\in MA} \max\{V_{NS};\ 0\} - \max\{C_{MA};0\};\ 0\right\} + \max\left\{\sum_{NS\in MA} \min\{V_{NS};\ 0\} - \min\{C_{MA};0\};\ 0\right\}$$

where:

the summation $NS\in MA$ is across the netting sets covered by the relevant margin agreement

V_{NS} is the current mark-to-market value of the netting set NS

C_{MA} is the cash equivalent value of all the currently available collateral in terms of the relevant margin agreement

(G) when the bank obtained eligible collateral which is taken outside a netting set, but is available to the bank to offset losses due to counterparty default on one netting set only, the bank shall treat such collateral as an independent collateral amount associated with the netting set and used within the calculation of replacement cost in terms of the provisions of item (E) above when the netting set is unmargined and in terms of the provisions of item (D) above when the netting set is margined, provided that-

(i) the bank shall treat any eligible collateral which is taken outside a netting set and that is available to the bank to offset losses due to counterparty default on more than one netting set as collateral taken under a margin agreement applicable to multiple netting sets, as envisaged in item (F) above;

(ii) when eligible collateral is available to offset losses on non-derivatives exposures as well as exposures determined using the standardised approach set out in this subregulation (18), the bank shall only use that portion of the collateral assigned to the derivatives to reduce the bank's relevant exposure to derivative instruments;

(H) in all cases the relevant exposure amount or EAD for a margined netting set shall be capped at the relevant exposure amount or EAD of the same netting set calculated on an unmargined basis;

(iii) shall calculate the relevant potential future exposure add-on component of the formula specified in subparagraph (i) above in accordance with the relevant requirements specified in this subparagraph (iii), provided that-

(A) for purposes of these Regulations-

(i) the relevant potential future exposure add-on shall consist of two distinct components, namely-

(aa) an aggregate add-on component-

(i) which consists of add-ons calculated for each relevant asset class within a given netting set, that is, the bank shall calculate the relevant add-on for each asset class through the application of the relevant specified asset-class-specific formulae that represent a stylised Effective EPE calculation under the assumption that all trades in the asset class have zero current mark-to-market value, that is, all trades are assumed to be at-the-money;

(ii) which add-on varies, based on the number of hedging sets that are available within an asset class, and which variations account for basis risk and differences in correlations within the relevant asset classes;

and

(bb) a multiplier that allows for the recognition of excess collateral or negative mark-to-market value for the relevant transactions;

(ii) the relevant potential future exposure may be stated mathematically as:

Potential future exposure (PFE) = multiplier * $AddOn^{aggregate}$

where:

multiplier	is a function of three inputs: V, C and $AddOn^{aggregate}$, which multiplier shall be subject to a floor of 5 per cent of the relevant PFE add-on
$AddOn^{aggregate}$	is the aggregate add-on component

(iii) the bank shall duly separate all relevant trades within each relevant asset class into the relevant required hedging sets and aggregate all the relevant trade-level inputs at the hedging set level and finally at the asset-class level, in accordance with the relevant formulae and requirements specified in this subparagraph (iii);

(iv) in the case of interest rate derivative instruments-

(aa) a hedging set shall consist of all relevant derivatives that reference interest rates of the same currency, such as, for example, ZAR, USD, EUR, JPY, etc., that is, there shall be a separate hedging set in respect of each relevant currency;

(bb) hedging sets shall be further divided into maturity categories in respect of which long and short positions in the same hedging set may fully offset each other within maturity categories, but only partial offsetting shall be permitted across maturity categories;

(v) in the case of foreign exchange derivative instruments, a hedging set shall consist of all relevant derivatives that reference the same foreign exchange currency pair, such as, for example, USD/ZAR, USD/Yen, Euro/Yen, or USD/Euro, that is, there shall be a separate hedging set in respect of each relevant currency pair, in respect of which full offsetting shall be permitted for long and short positions in the same currency pair, but no offsetting shall be permitted across currency pairs;

(vi) in the case of credit derivative instruments and equity derivative instruments, a single hedging set shall apply for each relevant asset class, in respect of which full offsetting shall be permitted for derivatives that reference the same entity (name or index), but only partial offsetting shall be permitted between derivatives referencing different entities;

(vii) in the case of commodity derivative instruments, four hedging sets shall apply, one for each different class of commodity, that is, one each for

energy, metals, agricultural, and other commodities, and in respect of which-

(aa) full offsetting shall be permitted between derivatives referencing the same commodity within the same hedging set;

(bb) partial offsetting shall be permitted between derivatives referencing different commodities; and

(cc) no offsetting shall be permitted between different hedging sets;

(viii) in respect of each relevant asset class, basis transactions and volatility transactions shall form separate hedging sets within their respective asset classes, as set out below, in respect of which the relevant specified factors shall apply:

All relevant-

(aa) derivatives that reference the basis between two risk factors and are denominated in a single currency, which shall for purposes of this subregulation (18) be referred to as basis transactions, shall be treated within separate hedging sets within the relevant corresponding asset class, that is, all basis transactions of a netting set that belong to the same asset class and reference the same pair of risk factors shall form a single hedging set, provided that-

(i) derivatives with two floating legs that are denominated in different currencies, such as, for example, cross-currency swaps, shall be treated as non-basis foreign exchange contracts;

(ii) within each relevant hedging set, long and short positions shall be determined with respect to the relevant basis;

(iii) the bank shall in the case of hedging sets that consist of basis transactions multiply the relevant specified factor denoted by $SF_i^{(a)}$, applicable to a given asset class, by one-half;

(bb) derivatives that reference the volatility of a risk factor, which shall for purposes of this subregulation (18) be referred to as volatility transactions, shall be treated within separate hedging sets within the relevant corresponding asset class, that is, all equity volatility transactions, for example, shall form a single hedging set, provided that the bank shall in the case of hedging sets that consist of volatility transactions multiply the relevant specified factor denoted by $SF_i^{(a)}$, applicable to a given asset class, by a factor of five;

(ix) the bank shall determine and allocate the primary risk factor or factors in respect of each relevant transaction to one or more of the following five asset classes:

(aa) interest rate;

(bb) foreign exchange;

(cc) credit;

(dd) equity; or

(ee) commodity;

(x) the bank shall allocate all its relevant derivative transactions to an appropriate asset class based on its primary risk driver or reference underlying instrument, such as, for example, an interest rate curve for an interest rate swap, a reference entity for a credit default swap, or a foreign exchange rate for a FX call option, provided that-

(aa) in the case of more complex trades that may have more than one

risk driver, such as, for example, multi-asset or hybrid derivatives, the bank shall take into account the relevant sensitivities and volatility of the underlying to determine the relevant primary risk driver;

(bb) subject to such conditions as may be specified in writing by the Authority, the Authority may direct the bank to allocate complex trades to more than one asset class, which will result in the same position being included in multiple asset classes, in which case the bank shall determine the appropriate sign and delta adjustment of the relevant risk driver for each relevant asset class to which the position is allocated;

(xi) the bank shall in all relevant cases calculate an adjusted notional amount based on the actual notional amount or price of the transaction, at the trade level, provided that-

(aa) in the case of interest rate derivative instruments or credit derivative instruments, the said trade-level adjusted notional amount for trade i of asset class a, which is denoted by $\mathbf{d}_i^{(a)}$-

(i) shall duly take into account both the size of a position and its maturity dependency, if any;

(ii) shall incorporate any relevant specified measure of duration;

(iii) shall be the product of the trade notional amount, converted to the relevant domestic currency, and the relevant specified duration, which is denoted by SD_i, and calculated through the application of the formula specified below:

$$SD_i = \frac{\exp(-0.05*S_i) - \exp(-0.05*E_i)}{0.05}$$

where:

S_i and E_i are the respective start and end dates of the time period referenced by the interest rate or credit derivative, or, where such a derivative references the value of another interest rate or credit instrument, the time period determined on the basis of the relevant underlying instrument, subject to a floor of ten business days, provided that when the start date has already occurred, such as, for example, an ongoing interest rate swap, S_i shall be equal to zero.

For example, a European interest rate swaption with expiry of 1 year and the term of the underlying swap of 5 years has a start date (S_i) of 1 year and an end date (E_i) of 6 years;

(bb) in the case of foreign exchange derivative instruments, the adjusted notional amount shall be the notional amount of the relevant foreign currency leg of the contract, converted to the relevant domestic currency, provided that when both legs of the foreign exchange derivative transaction are denominated in currencies other than the relevant domestic currency, the bank shall convert the notional amount of each leg to the relevant domestic currency and the leg with the larger domestic currency value shall be the adjusted notional amount;

(cc) in the case of equity and commodity derivative instruments, the adjusted notional amount shall be equal to the product of the

current price of one unit of the stock or commodity, such as, for example, a share of equity or barrel of oil, and the number of units referenced by the trade;

(dd) when the trade notional amount is not stated clearly in the relevant contract, and fixed until maturity-

(i) and the notional is a formula of market values, the bank shall apply the current market values to determine the relevant required trade notional amount;

(ii) the bank shall in the case of interest rate and credit derivative contracts with variable notional amounts specified in the contract, such as amortising and accreting swaps, use the relevant time-weighted average notional over the remaining life of the derivative as the relevant required trade notional amount,

Provided that the aforementioned requirements related to averaging do not apply to transactions in respect of which the notional varies due to price changes, such as, for example, foreign exchange, equity and commodity derivative contracts.

(iii) the bank shall in the case of leveraged swaps, convert the relevant value to the notional of an equivalent unleveraged swap.

For example, when all rates in a swap are multiplied by a factor, the bank shall multiply the stated notional amount by that factor on the interest rates to determine the relevant required trade notional amount;

(iv) the bank shall in the case of a derivative contract with multiple exchanges of principal, multiply the notional amount with the number of exchanges of principal in the derivative contract to determine the relevant required trade notional amount;

(v) the remaining maturity of a derivative contract that is structured such that on specified dates any outstanding exposure is settled and the terms are reset so that the fair value of the contract is zero, shall be the time until the next reset date;

(ee) depending on whether the relevant transaction is a margined or an unmargined transaction, the bank shall apply to the relevant adjusted notional amount any relevant specified maturity factor, at the trade level, to duly reflect the time horizon appropriate for the relevant type of transaction;

(ff) based upon the relevant long or short position and whether the trade is an option, CDO tranche or neither, the bank shall apply to the relevant trade-level adjusted notional amount any relevant specified delta adjustment as envisaged in sub-item (xii) below, in order to determine an effective notional amount':

Provided that in the case of single-payment options the bank shall calculate the relevant required effective notional amount, that is, $D = d * MF * \delta$, as follows:

(i) For European, Asian, American and Bermudan put and call options, the bank shall calculate the required delta by using the simplified Black-Scholes formula specified in sub-item (xii) below. In the case of Asian options, the underlying price must be set equal to the current value of the average used in the payoff. In the case of American and Bermudan options, the bank shall use the latest allowed exercise date as the exercise date T_i in the relevant specified formula;

(ii) For Bermudan swaptions, the start date S_i shall be equal to the earliest allowed exercise date, and the end date E_i shall be equal to the end date of the underlying swap;

(iii) For digital options, the bank shall approximate the payoff of each bought or sold digital option with strike K_i via the "collar" combination of bought and sold European options of the same type, that is, call or put, with the strikes set equal to $0.95 \cdot K_i$ and $1.05 \cdot K_i$. The size of the position in the collar components must be such that the digital payoff is reproduced exactly outside the region between the two strikes. The bank shall then separately compute the effective notional for the bought and sold European components of the collar, using the option formulae for the delta envisaged in sub-item (xii), and by using the exercise date T_i and the current value of the underlying P_i of the said digital option. The bank shall cap the absolute value of the digital-option effective notional by the ratio of the digital payoff to the relevant specified factor;

(iv) When a trade's payoff can be represented as a combination of European option payoffs, such as, for example, collar, butterfly/calendar spread, straddle, strangle, each relevant European option component shall be treated as a separate trade.

For the purpose of calculating the relevant required effective notional amounts, multiple-payment options may be represented as a combination of single-payment options. In particular, interest rate caps/floors may be represented as the portfolio of individual caplets/floorlets, each of which is a European option on the floating interest rate over a specific coupon period. For each relevant caplet/floorlet, S_i and T_i shall be the time periods starting from the current date to the start of the coupon period, while E_i shall be the time period starting from the current date to the end of the relevant coupon period;

(gg) in order to duly reflect volatility, the bank shall apply to each relevant effective notional amount such volatility factor as envisaged in sub-item (xiii) below;

(xii) the bank shall apply to the aforesaid adjusted notional amount the relevant specified delta adjustment, at the trade level, to duly reflect the relevant direction of the transaction and its non-linearity, which delta adjustment is defined as follows:

δ_i	**Long in the primary risk factor[1]**	**Short in the primary risk factor[2]**
Instruments other than options or CDO tranches	+1	-1

1. **Means the market value of the instrument increases when the value of the primary risk factor increases.**
2. **Means the market value of the instrument decreases when the value of the primary risk factor increases.**

δ_i	**Bought[1]**
Call Options[1]	$+\Phi\left(\frac{\ln(P_i / K_i) + 0.5 * \sigma_i^2 * T_i}{\sigma_i * \sqrt{T_i}}\right)$
Put Options[1]	$-\Phi\left(-\frac{\ln(P_i / K_i) + 0.5 * \sigma_i^2 * T_i}{\sigma_i * \sqrt{T_i}}\right)$
δ_i	**Sold[1]**

Call Options[1]	$-\Phi\left(\frac{\ln(P_i / K_i) + 0.5 * \sigma_i^2 * T_i}{\sigma_i * \sqrt{T_i}}\right)$
Put Options[1]	$+\Phi\left(-\frac{\ln(P_i / K_i) + 0.5 * \sigma_i^2 * T_i}{\sigma_i * \sqrt{T_i}}\right)$
In respect of which the bank shall determine: P_i: the underlying price (spot, forward, average, etc) K_i: the strike price T_i: the latest contractual exercise date of the option The specified volatility σ_i of an option	

1. **The symbol Φ in these equations represents the standard normal cumulative distribution function.**

δ_i	**Purchased (long protection)**
CDO tranches	$+\frac{15}{(1+14*A_i) * (1+14*D_i)}$
δ_i	**Sold (short protection)**
CDO tranches	$-\frac{15}{(1+14*A_i) * (1+14*D_i)}$
In respect of which the bank shall determine: A_i: the attachment point of the CDO tranche D_i: the detachment point of the CDO tranche	

(xiii) in order to convert the relevant effective notional amount into an Effective EPE based on the measured volatility of the asset class, the bank shall apply to the aforesaid amount any relevant factor or factors specific to each asset class, which factor(s) is denoted by $SF_i^{(a)}$ and has been calibrated to reflect the Effective EPE of a single at-the-money linear trade of unit notional and one-year maturity, in accordance with the relevant requirements specified in this subparagraph (iii);

(xiv) in the case of-

(aa) margined transactions-

(i) the bank shall determine the minimum margin period of risk in accordance with the relevant requirements specified in table 1 below:

Table 1

Minimum margin period of risk	
Non-centrally-cleared derivative transactions subject to daily margin agreements	At least 10 business days
Centrally cleared derivative transactions subject to daily margin agreements between clearing members and their clients	5 business days
Netting sets consisting of 5,000 transactions that are not with a central counterparty	20 business days
Netting sets with outstanding disputes as envisaged in subregulation (19)(e)(ii)	Double the relevant specified margin period of risk

(ii) the bank shall multiply the relevant adjusted notional amount at the trade level by:

$$MF_i^{(margined)} = \frac{3}{2}\sqrt{\frac{MPOR_i}{1\ year}}$$

where:

$MPOR_i$ is the margin period of risk appropriate for the relevant margin agreement containing the transaction i.

(bb) unmargined transactions-

(i) the minimum time risk horizon shall be the lesser of one year and the remaining maturity of the relevant derivative contract, subject to a floor of ten business days;

(ii) the bank shall multiply the relevant adjusted notional amount at the trade level by:

$$MF_i^{(unmargined)} = \sqrt{\frac{\min\{M_i; 1\ year\}}{1\ year}}$$

where:

M_i is the remaining maturity of transaction i, subject to a floor of ten business days

(xv) in the case of credit derivative instruments, equity derivative instruments and commodity derivative instruments, the bank shall apply to the relevant PFE add-on calculation the relevant specified correlation parameters, denoted by $\rho_i^{(a)}$, to determine the appropriate degree of offset between individual trades in respect of the systemic and idiosyncratic components;

(xvi) in order to determine the relevant date(s) to be applied-

(aa) the maturity of a contract, denoted by Mi, shall in all cases be the latest date that the contract may still be active, provided that when a derivative contract has another derivative contract as its underlying, such as, for example, a swaption, that may be exercised into the relevant underlying contract, that is, the bank would assume a position in the underlying contract in the event of exercise, then the maturity of that contract shall be the final settlement date of the relevant underlying derivative contract;

(bb) in the case of interest rate and credit derivative instruments, the start date and the end date of the relevant time period, respectively denoted by S_i and E_i, shall be determined in accordance with the relevant dates specified in the contract, provided that when the derivative references the value of another interest rate or credit instrument, such as, for example, a swaption or bond option, the bank shall determine the relevant maturity category or time period based on the relevant underlying instrument;

(cc) in the case of options, the latest contractual exercise date, denoted by T_i, shall be determined based on the relevant date specified in the contract, which period shall also be used to determine any relevant delta value;

(xvii) the respective dates envisaged in subitem (xvi) above related to specified example types of transaction are set out in table 1 below:

Table 1

Instrument	M_i	S_i	E_i
Interest rate or credit default swap maturing in 10 years	10 years	0	10 years
10-year interest rate swap, forward starting in 5	15	5 years	15

years	years		years
Forward rate agreement for time period starting in 6 months and ending in 12 months	1 year	0.5 year	1 year
Cash-settled European swaption referencing 5-year interest rate swap with exercise date in 6 months	0.5 year	0.5 year	5.5 years
Physically-settled European swaption referencing 5-year interest rate swap with exercise date in 6 months	5.5 years	0.5 year	5.5 years
10-year Bermudan swaption with annual exercise dates	10 years	1 year	10 years
Interest rate cap or floor specified for semi-annual interest rate with maturity 5 years	5 years	0	5 years
Option on a bond maturing in 5 years with the latest exercise date in 1 year	1 year	1 year	5 years
3-month Eurodollar futures that matures in 1 year	1 year	1 year	1.25 years
Futures on 20-year treasury bond that matures in 2 years	2 years	2 years	22 years
6-month option on 2-year futures on 20-year treasury bond	2 years	2 years	22 years

(xviii) the respective parameters to be applied in the required calculations of the respective add-on components envisaged in this subparagraph (iii) are set out in table 1 below:

Table 1

Asset class	Subclass	Specified factor[1; 2] $SF_i^{(a)}$	Correlation $\rho_i^{(a)}$	Option volatility
Interest rate		0.50%	N/A	50%
Foreign exchange		4.0%	N/A	15%
Credit, single name	AAA	0.38%	50%	100%
	AA	0.38%	50%	100%
	A	0.42%	50%	100%
	BBB	0.54%	50%	100%
	BB	1.06%	50%	100%
	B	1.6%	50%	100%
	CCC	6.0%	50%	100%
Credit, index	IG[3]	0.38%	80%	80%
	SG[4]	1.06%	80%	80%
Equity, single name		32%	50%	120%
Equity, index		20%	80%	75%
Commodity	Electricity	40%	40%	150%
	Oil/Gas	18%	40%	70%
	Metals	18%	40%	70%
	Agricultural	18%	40%	70%
	Other	18%	40%	70%

1. **The bank shall in the case of a basis transaction hedging set multiply the relevant specified factor applicable to the relevant asset class by one-half.**
2. **The bank shall in the case of a volatility transaction hedging set multiply the relevant specified factor applicable to the relevant asset class by a factor of five.**
3. **Means investment grade.**
4. **Means speculative grade.**

(B) when the bank enters into multiple margin agreements that apply to a single netting set, the bank shall divide the netting set into sub-netting sets that align with their respective margin agreement;

(C) when a single margin agreement applies to several netting sets, as envisaged in subparagraph (ii)(F) above, and collateral is exchanged based on the mark-to-market values that are netted across all relevant transactions covered under the margin agreement, irrespective of the netting sets, and as such the collateral exchanged on a net basis may not be sufficient to cover the potential future exposure, the bank shall-

(i) calculate the PFE add-on in accordance with the unmargined methodology;

(ii) aggregate the netting set level PFEs through the application of the formula specified below:

$$PFE_{MA} = \sum_{NS \in MA} PFE_{NS}^{(unmargined)}$$

where:

$PFE_{NS}^{(unmargined)}$ is the PFE add-on for the netting set NS calculated in accordance with the relevant requirements related to unmargined transactions

(D) based on the aforesaid, in the case of interest rate derivative instruments-

(i) the relevant add-on-

(aa) shall be equal to the sum of the add-ons for each relevant hedging set transacted with a counterparty in a netting set;

(bb) is intended to capture the risk of imperfect correlation between interest rate derivatives of different maturities;

(cc) for a hedging set shall be calculated in two steps, as set out in subitems (iv) to (vii) below;

(ii) based on the end-date of the relevant transactions, the bank shall allocate all relevant transactions into one of the following three maturity categories:

(aa) less than one year;

(bb) between one year and five years; and

(cc) more than five years;

(iii) the bank may-

(aa) fully offset all relevant positions within a relevant specified maturity category; and

(bb) partially offset relevant positions across the relevant specified maturity categories in accordance with the relevant requirements specified in this subparagraph (iii);

(iv) the bank shall firstly calculate the effective notional amount for time bucket k of hedging set j, that is, currency j, through the application of the formula specified below:

$$D_{jk}^{(IR)} = \sum_{i \in \{Ccy_j, MB_k\}} \delta_i * d_i^{(IR)} * MF_i^{(type)}$$

where:

$D_{jk}^{(IR)}$ is the effective notional amount

$i \in \{Ccy_j, MB_k\}$ refers to trades of currency j that belong to maturity bucket k

That is, the effective notional for each relevant time bucket and currency shall be equal to the sum of the trade-level adjusted notional amounts multiplied by-

(aa) the relevant delta adjustments; and

(bb) the relevant maturity factor,

specified hereinbefore;

(v) when the bank wishes-

(aa) to offset relevant positions across maturity buckets, the bank shall, as part of the second step, aggregate across the relevant maturity buckets for each relevant hedging set through the application of the formulae specified below:

$$\text{EffectiveNotional}_{j}^{(IR)} = \left[\left(D_{j1}^{(IR)}\right)^2 + \left(D_{j2}^{(IR)}\right)^2 + \left(D_{j3}^{(IR)}\right)^2 + A + B + C\right]^{\frac{1}{2}}$$

where:

$$A = 1.4 * D_{j1}^{(IR)} * D_{j2}^{(IR)}$$

$$B = 1.4 * D_{j2}^{(IR)} * D_{j3}^{(IR)}$$

$$C = 0.6 * D_{j1}^{(IR)} * D_{j3}^{(IR)}$$

(bb) not to offset positions across maturity buckets, the bank shall, as part of the second step, calculate the relevant effective notional amount through the application of the formula specified below:

$$\text{EffectiveNotional}_{j}^{(IR)} = \left|D_{j1}^{(IR)}\right| + \left|D_{j2}^{(IR)}\right| + \left|D_{j3}^{(IR)}\right|$$

(vi) the bank shall thereafter, as part of the second step, calculate the hedging set level add-on as the product of the effective notional and the relevant specified interest rate factor, through the application of the formula specified below:

$$\text{AddOn}_{j}^{(IR)} = SF_{j}^{(IR)} * \text{EffectiveNotional}_{j}^{(IR)}$$

(vii) the bank shall then finally, as part of the second step, aggregate the said hedging set level add-ons by means of simple summation, through the application of the formula specified below:

$$\text{AddOn}^{(IR)} = \sum_{j} \text{AddOn}_{j}^{(IR)}$$

(E) based on the aforesaid, in the case of foreign exchange derivative instruments-

(i) the add-on for a hedging set shall be the product of the absolute value of the relevant effective notional amount and the relevant specified factor, which is the same for all relevant FX hedging sets;

(ii) the relevant effective notional amount of a hedging set shall be equal to the sum of all the relevant trade-level adjusted notional amounts multiplied by the relevant specified delta value;

(iii) the adjusted notional amount is maturity independent and equal to the notional amount of the relevant foreign currency leg of the contract, converted to Rand;

(iv) the add-on shall be calculated through the application of the formula specified below:

$$\text{AddOn}^{(FX)} = \sum_{j} \text{AddOn}_{HS_j}^{(FX)}$$

where:

the sum is taken over all the relevant hedging sets, denoted by HS_j, included in the relevant netting set.

the add-on and the effective notional of the hedging set HS_j are respectively calculated through the application of the formulae specified below:

$$AddOn_{HS_j}^{(FX)} = SF_j^{(FX)} * \left| EffectiveNotional_j^{(FX)} \right|$$

$$EffectiveNotional_j^{(FX)} = \sum_{i \in HS_j} \delta_i * d_i^{(FX)} * MF_i^{(type)}$$

where:

$i \in HS_j$ means the relevant trades related to hedging set HS_j

that is, the effective notional for each relevant currency pair shall be equal to the sum of the relevant trade-level adjusted notional amounts multiplied by-

(aa) the relevant delta adjustment; and

(bb) the relevant maturity factor,

specified hereinbefore;

(F) based on the aforesaid, in the case of credit derivative instruments-

(i) the bank shall firstly calculate an entity-level effective notional amount in respect of all relevant credit derivative instruments referencing either the same single entity or an index, in respect of which the bank may fully offset all relevant credit derivative instruments referencing that same single entity or index, through the application of the formula specified below:

$$EffectiveNotional_k^{(Credit)} = \sum_{i \in Entity_k} \delta_i * d_i^{(Credit)} * MF_i^{(type)}$$

where:

$i \in Entity_k$ means the relevant trades related to entity k

that is, the effective notional for each relevant entity shall be equal to the sum of the relevant trade-level adjusted notional amounts multiplied by-

(aa) the relevant delta adjustment; and

(bb) the relevant maturity factor,

specified hereinbefore;

(ii) the bank shall thereafter calculate the add-on for all the relevant positions referencing the aforesaid entity or index, through the application of the formula specified below:

$$AddOn(Entity_k) = SF_k^{(Credit)} * EffectiveNotional_k^{(Credit)}$$

that is, the add-on for all the relevant positions referencing the aforesaid entity shall be the product of its effective notional amount and the relevant specified factor,

where:

$SF_k^{(Credit)}$ is the relevant specified factor, which shall be determined as follows:

(aa) in the case of any single name entity, based on the credit rating of the relevant reference entity;

and

(bb) in the case of any relevant index entity, based on whether that index is investment grade or speculative grade;

(iii) with the exception of all relevant basis and volatility transactions, the bank shall then-

(aa) group all the relevant entity-level add-ons within a single hedging set, in which full offsetting between two different entity-level add-ons shall not be permitted.

Instead, a single-factor model is used that make provision for partial offsetting between the entity-level add-ons by dividing the risk of the credit derivatives asset class into a systemic component and an idiosyncratic component. The entity-level add-ons may fully offset each other in the systemic component, but no offsetting benefit is permitted in the idiosyncratic component.

The aforesaid two components are weighted by a correlation factor that determines the degree of offsetting/hedging benefit within the relevant credit derivatives asset class. The higher the correlation factor, the higher the importance of the systemic component, hence the higher the degree of offsetting benefits. Derivatives referencing credit indices shall be treated as though they were referencing single names, but a higher correlation factor applies;

(bb) calculate the relevant add-on through the application of the formula specified below:

$$AddOn^{(Credit)} = [A + B]^{½}$$

where:

$$A = \left(\sum_k \rho_k^{(Credit)} * AddOn(Entity_k)\right)^2$$

$$B = \sum_k \left(1 - (\rho_k^{(Credit)})^2\right) * (AddOn(Entity_k))^2$$

$\rho_k^{(Credit)}$ is the relevant correlation factor specified for Entity k

(G) based on the aforesaid, in the case of equity derivative instruments-

(i) the bank shall firstly calculate an entity-level effective notional amount in respect of each relevant reference entity or index, in respect of which the bank may fully offset all relevant transactions related to the same reference entity or index, through the application of the formula specified below:

$$EffectiveNotional_k^{(Equity)} = \sum_{i \in Entity_k} \delta_i * d_i^{(Equity)} * MF_i^{(type)}$$

where:

$i \in Entity_k$ means the relevant trades related to entity k

that is, the effective notional for each relevant entity shall be equal to the sum of the relevant trade-level adjusted notional amounts multiplied by-

(aa) the relevant delta adjustment; and

(bb) the relevant maturity factor,

specified hereinbefore;

(ii) the bank shall thereafter calculate the add-on for all the relevant positions referencing the aforesaid entity or index, through the application of the formula specified below:

$$AddOn(Entity_k) = SF_k^{(Equity)} * EffectiveNotional_k^{(Equity)}$$

that is, the add-on for all the relevant positions referencing the aforesaid entity or index shall be the product of its effective notional amount and the relevant specified factor,

where:

$SF_k^{(Equity)}$ is the relevant specified factor

(iii) the bank shall then-

(aa) group all the relevant entity-level add-ons, in which full offsetting between two different entity-level add-ons shall not be permitted.

Instead, a single-factor model is used to divide the risk into a systemic component and an idiosyncratic component in respect of each relevant reference entity or index. The entity-level add-ons may fully offset each other in the systemic component, but no offsetting benefit is permitted in the idiosyncratic component.

The aforesaid two components are weighted by a correlation factor which determines the degree of offsetting/hedging benefit. Derivatives referencing equity indices shall be treated as though they were referencing single entities, but a higher correlation factor applies for the systemic component;

(bb) calculate the relevant add-on through the application of the formula specified below:

$$AddOn^{(Equity)} = [A + B]^{½}$$

where:

$$A = \left(\sum_k \rho_k^{(Equity)} * AddOn(Entity_k)\right)^2$$

$$B = \sum_k \left(1 - (\rho_k^{(Equity)})^2\right) * (AddOn(Entity_k))^2$$

$\rho_k^{(Equity)}$ is the relevant correlation factor specified for Entity k

(H) based on the aforesaid, in the case of commodity derivative instruments-

(i) the bank-

(aa) may in the calculation of the commodity type-level effective notional amount fully offset all relevant derivative transactions referencing the same type of commodity;

(bb) shall calculate the effective notional amount of the commodity type k in hedging set j, through the application of the formula specified below:

$$EffectiveNotional_k^{(Com)} = \sum_{i \epsilon Type_k^j} \delta_i * d_i^{(Com)} * MF_i^{(type)}$$

where:

$i \epsilon Type_k^j$ refers to the trades of commodity type k in hedging set j

that is, the effective notional amount for each relevant commodity type shall be equal to the sum of the relevant trade-level adjusted notional amounts multiplied by-

(i) the relevant delta adjustment; and

(ii) the relevant maturity factor,

specified hereinbefore;

(ii) the bank shall then calculate the add-on for the relevant commodity type k in hedging set j, through the application of the formula specified below:

$$AddOn(Type_k^j) = SF_{Type_k^j}^{(Com)} * EffectiveNotional_k^{(Com)}$$

(iii) within each relevant hedging set-

(aa) a single factor model is used to divide the risk of the same type of commodities into a systemic component and an idiosyncratic component, in terms of which partial offsetting/hedging benefits is allowed within each relevant hedging set between the same type of commodities, but no offsetting/hedging benefits shall be applied between the respective hedging sets;

(bb) the bank shall calculate the relevant add-on through the application of the formula specified below:

$$AddOn_{HSj}^{(Com)} = [A + B]^{½}$$

where:

$$A = \left(\rho_j^{(Com)} * \sum_k AddOn(Type_k^j)\right)^2$$

$$B = \left(1 - (\rho_j^{(Com)})^2\right) * \sum_k \left(AddOn(Type_k^j)\right)^2$$

$\rho_j^{(Com)}$ is the relevant correlation factor in respect of hedging set j

(iv) the bank shall then finally calculate the add-on for the relevant asset class by means of simple summation, through the application of the formula specified below:

$$AddOn^{(Com)} = \sum_j AddOn_{HSj}^{(Com)}$$

where the sum is taken over all the relevant hedging sets;

(I) when the relevant amount of collateral held-

(i) is less than the net market value of the derivative contracts, that is, the position is under-collateralised, the current replacement cost is positive and the multiplier shall be equal to one, that is, the PFE component shall be equal to the full value of the aggregate add-on;

(ii) is more than the net market value of the derivative contracts, that is, the position is over-collateralised, the current replacement cost is equal to zero, and the multiplier shall be less than one, that is, the PFE component shall be less than the full value of the aggregate add-on;

(J) since out-of-the-money transactions do not represent a current exposure, and have less chance to go in-the-money, the aforesaid multiplier shall also be activated in the case of transactions with negative current value, that is, out-of-the-money transactions, which may be stated mathematically as:

$$\text{Multiplier} = \min\left\{1; \text{Floor} + (1 - \text{Floor}) * A\right\}$$

where:

$$A = \exp\left(\frac{V - C}{2 * (1 - \text{Floor}) * \text{AddOn}^{\text{aggregate}}}\right)$$

exp(...) equals to the exponential function

Floor is 5 per cent

V is the value of the derivative transactions in the relevant netting set

C is the haircut value of the net collateral held

(K) in all relevant cases, the relevant exposure amount or EAD in respect of a margined netting set shall be capped at the relevant exposure amount or EAD of the same netting set calculated on an unmargined basis;

(L) the bank shall in no case apply any diversification benefits across asset classes, that is, the bank shall calculate the potential future exposure add-on amount for each relevant asset class within a given netting set by simply aggregating the relevant amounts, which may be stated mathematically as:

$$\text{AddOn}^{\text{aggregate}} = \sum_{a} \text{AddOn}^{(a)}$$

(b) *Matters related to bilateral netting*

A bank that adopted the standardised approach for the measurement of the bank's exposure to counterparty credit risk may in the calculation of the relevant replacement cost component of a netting set, net transactions-

(i) subject to novation, in terms of which any obligation between the bank and its counterparty to deliver a given currency on a given value date is automatically amalgamated with all other obligations for the same currency and value date, legally substituting one single amount for the previous gross obligations; or

(ii) subject to any legally valid form of bilateral netting not included in subparagraph (i) above, including any other form of novation:

Provided that, in all relevant cases-

(A) the bank shall have in place a netting contract or agreement with the said counterparty that creates a single legal obligation, covering all included transactions, such that the bank would have either a claim to receive or an obligation to pay only the net sum of the positive and negative mark-to-market values of the said transactions in the event of counterparty failure to perform in accordance with the contractual agreement, irrespective whether or not the said failure relates to default, bankruptcy, liquidation or any other similar circumstances;

(B) the bank shall have in place written and reasoned legal opinions confirming that in the event of a legal challenge the relevant courts and administrative authorities would find the bank's exposure to be the said net amount in terms of-

(i) the law of the jurisdiction in which the counterparty is incorporated or chartered, and when the foreign branch of a counterparty is involved, also in terms of the law of the jurisdiction in which the branch is located;

(ii) the law that governs the individual transactions; and

(iii) the law that governs any contract or agreement necessary to effect the said novation or netting;

(C) when a national supervisor or regulator is not satisfied with the legal enforceability of the said agreement, neither counterparty shall apply netting in respect of the relevant transactions or contracts;

(D) the bank shall have in place robust procedures in order to continuously monitor the legal characteristics of the said netting agreement for possible changes in relevant law that may affect the legal enforceability of the said agreement;

(E) since the gross obligations are not in any way affected, no payment netting agreement, which is designed to reduce the operational costs of daily settlements, shall be taken into consideration in the calculation of the reporting bank's exposure amount, EAD or required capital and reserve funds;

(F) no contract containing walk-away clauses, that is, a provision that permits a non-defaulting counterparty to make only limited payments or no payment at all to the estate of a defaulter, even when the defaulter is a net creditor, shall be eligible for netting in terms of these Regulations.";

(m) by the substitution in subregulation (19) for the heading of the following heading:

"(19) *Calculation of counterparty credit exposure in terms of the internal model method*";

(n) by the substitution in subregulation (19)(e) for subparagraph (i) of the following subparagraph:

"(i) Subject to the provisions of subparagraphs (ii) and (iii) below, when a particular netting set is subject to a margin agreement and the reporting bank's internal model is able to capture the effect of margining in its estimation of expected exposure, the bank may apply for the approval of the Authority to directly use the said estimated expected exposure amount in the formula relating to effective expected exposure, specified in paragraph (a) above;";

(o) by the substitution in subregulation (19)(e)(ii) for item (E) of the following item:

"(E) in the case of re-margining with a periodicity of N-days, the bank shall apply a margin period of risk of at least the aforesaid specified floor plus the N days minus one day, that is:

Margin Period of Risk = F + N - 1.

where:

F is the floor number of days specified hereinbefore

N is the said periodicity of N-days for re-margining";

(p) by the substitution in subregulation (19)(h)(i)(A) for the description specified related to the variable EE_i of the following description:

"**EE_i** is the expected exposure to the counterparty at revaluation time t_i, as defined in paragraph (a) above, where exposures of different netting sets for such counterparty are added, and where the longest maturity of each netting set is given by the longest contractual maturity inside the netting set";

(q) by the substitution for subregulation (23) of the following subregulation:

"(23) Instructions relating to the completion of the monthly form BA 200 are furnished with reference to the headings and item descriptions of specified columns and line items appearing on the form BA 200, as follows:

Items relating to the summary of selected credit risk related information: standardised approach

Item number	Description
2	**Impaired advances** This item shall reflect the relevant aggregate amount of impaired advances. As a minimum, an advance is considered to be impaired when objective evidence exists that the bank is unlikely to collect the total amount due.
3 to 6	**Assets bought-in** These items shall reflect the relevant aggregate on-balance sheet carrying value of assets bought-in during the preceding five years to protect an investment, including a loan or advance, which assets have not been disposed of at the end of the reporting period.

7 to 9	**Credit impairment** These items shall reflect the respective relevant required aggregate amounts of specific credit impairments and portfolio credit impairments raised by the reporting bank in accordance with the relevant requirements specified in Financial Reporting Standards issued from time to time.
11	**Total gross credit exposure** This item shall reflect the relevant required gross amount of credit exposure before the application of credit risk mitigation and any relevant credit conversion factor.
12	**Credit exposure value post credit risk mitigation** This item shall reflect the relevant required aggregate amount of gross credit exposure after the effect of any relevant credit risk mitigation has been included.
13	**Credit exposure post credit risk mitigation and credit conversion** This item shall reflect the relevant required aggregate amount of gross credit exposure after the effects of any relevant credit risk mitigation and credit conversion factors have been included.

Columns relating to summary of on-balance-sheet and off-balance-sheet credit exposure: standardised approach, items 14 to 34

Column number	Description
1	**On-balance-sheet exposure** This column shall reflect the relevant aggregate amount in respect of amounts drawn by clients, that is, utilised amounts, which amounts form part of the current exposure of the reporting bank, before the impact of any relevant credit risk mitigation has been taken into consideration.
2	**Off-balance-sheet exposure** This column shall reflect the relevant aggregate amount relating to, for example, exposures in respect of which a facility has been granted by the reporting bank to an obligor but in respect of which no funds have been paid out and no debit balance has been created, other than any exposure arising from a derivative instrument or repo-style transaction, including any exposure amount in respect of an irrevocable commitment, prior to the application of any relevant credit conversion factor or credit risk mitigation.
3	**Repurchase and/ or resale agreements** This column shall reflect the relevant aggregate amount in respect of any credit exposure arising from a repurchase and/ or resale agreement concluded by the reporting bank.
4	**Derivative instruments** This column shall reflect the relevant aggregate amount in respect of any credit exposure arising from derivative instruments, including any relevant exposure amount relating to counterparty credit risk.
14	**Credit exposure post credit risk mitigation** This column shall reflect the relevant required aggregate amount of gross credit exposure after the impact of any relevant credit risk mitigation has been taken into consideration.

Items relating to reconciliation of credit impairment: standardised approach

Item number	Description
40	**Interest in suspense** Since interest income related to impaired loans may not ultimately contribute to income when doubt exists regarding the recovery of the relevant loan amount or related interest amount due, this item shall reflect the relevant amount of interest in suspense, that is, irrespective of the accounting treatment of interest income from time to time, this item shall reflect the difference between the relevant amount of interest contractually due to the reporting bank by its clients up to the end of the reporting month and the relevant amount of interest income actually included in the operating profit or loss of the bank.
43	**Recoveries** This item shall reflect the relevant aggregate amount in respect of recoveries,

	net of any relevant amount relating to specific credit impairment and/ or portfolio credit impairment.

Columns relating to credit capital requirements based on risk weights: standardised approach, items 47 to 69

Column number	Description
1	**Total gross credit exposure** This column shall reflect the relevant aggregate gross credit exposure amount relating to the reporting bank's- (a) on-balance-sheet exposure, gross of any valuation adjustment or credit impairment; (b) off-balance-sheet exposure, including amounts in respect of irrevocable commitments, prior to the application of any credit-conversion factor; (c) exposure in respect of any repurchase or resale agreement; (d) exposure in respect of derivative instruments, calculated in accordance with the relevant requirements specified in subregulations (15) to (19).
2	**Specific credit impairment** This column shall reflect the relevant aggregate amount relating to any specific credit impairment in respect of the exposure amount reported in column 1.
3	**Exposure amount post credit risk mitigation (CRM) and specific credit impairment** This column shall reflect the reporting bank's relevant adjusted exposure amount, that is, the relevant amount net of any credit risk mitigation and specific credit impairment, calculated in accordance with the relevant requirements specified in these Regulations.
4 to 10	**Breakdown of off-balance-sheet exposure based on credit conversion factors (CCF)** Based on the relevant credit conversion factors specified in subregulation (6)(g), these columns shall reflect the appropriate breakdown of the reporting bank's adjusted exposure, that is, amounts included in column 3, relating to off-balance-sheet exposure.

Columns relating to counterparty credit risk based on specified risk weights: standardised approach, items 80 to 85

Column number	Description
1	**Replacement cost: OTC derivative instruments - unmargined transactions** In respect of unmargined transactions in OTC derivative instruments, this column shall reflect the relevant loss amount that would occur if a counterparty were to default and all relevant transactions were to be closed out immediately.
2	**Potential future exposure - add on: OTC derivative instruments: unmargined transactions** In respect of unmargined transactions in OTC derivative instruments, this column shall reflect the potential increase in exposure over a one-year time horizon from the relevant reporting date.
3	**Replacement cost: OTC derivative instruments - margined transactions** In respect of margined transactions in OTC derivative instruments, this column shall reflect the relevant loss amount that would occur if a counterparty were to default, assuming that the closeout and replacement of transactions occur instantaneously.
4	**Potential future exposure - add on: OTC derivative instruments: margined transactions** In respect of margined transactions in OTC derivative instruments, this

	column shall reflect the potential change in value of the relevant trades between the last exchange of collateral before default and replacement of the trades in the market, that is the margin period of risk.
5	**Credit exposure value** In the absence of an eligible master netting agreement, this column shall reflect the current value of all relevant credit exposures arising from securities financing transactions, after the effect of any relevant haircut has been taken into consideration.
6	**Collateral value** In the absence of an eligible master netting agreement, this column shall reflect the current value of eligible financial collateral obtained by the reporting bank in respect of all relevant securities financing transactions, after the effect of any relevant haircut has been taken into consideration.
7	**Netting benefit** This column shall reflect the aggregate amount of all relevant netting benefits arising from eligible master netting agreements taken into consideration in the calculation of the reporting bank's relevant adjusted credit exposure amount arising from securities financing transactions.
8	**Effective expected positive exposure** Based on the relevant requirements specified in subregulation (19)(a), this column shall reflect the relevant required effective expected positive exposure amount related to OTC derivative instruments.
9	**Stressed effective expected positive exposure** Based on the relevant requirements specified in, amongst others, subregulations (15) and (19) of these Regulations, this column shall reflect the relevant required effective expected positive exposure amount related to OTC derivative instruments in terms of a stressed scenario.
10	**Effective expected positive exposure** Based on the relevant requirements specified in subregulation (19)(a), this column shall reflect the relevant required effective expected positive exposure amount related to securities financing transactions.
11	**Stressed effective expected positive exposure** Based on the relevant requirements specified in, amongst others, subregulations (15) and (19) of these Regulations, this column shall reflect the relevant required effective expected positive exposure amount related to securities financing transactions in terms of a stressed scenario.
12	**Exposure amount: OTC derivative instruments – unmargined transactions** This column shall reflect the relevant required exposure or EAD amount in respect of unmargined transactions in OTC derivative instruments, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
13	**Exposure amount: OTC derivative instruments – margined transactions** This column shall reflect the relevant required exposure or EAD amount in respect of margined transactions in OTC derivative instruments, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
14	**Exposure amount - securities financing transactions** This column shall reflect the relevant required exposure or EAD amount in respect of securities financing transactions, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
15	**Default risk - OTC derivative instruments – unmargined transactions** This column shall reflect the relevant required risk weighted exposure amount in respect of unmargined transactions in OTC derivative instruments, calculated in terms of the relevant requirements specified in these

	Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
16	**Default risk - OTC derivative instruments – margined transactions** This column shall reflect the relevant required risk weighted exposure amount in respect of margined transactions in OTC derivative instruments, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
17	**Default risk - securities financing transactions** This column shall reflect the relevant required risk weighted exposure amount for securities financing transactions, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
18	**Standardised approach for CVA** Based on the relevant requirements specified in subregulation (15), this column shall reflect the relevant required risk weighted exposure amount for CVA risk, calculated in terms of the standardised approach, provided that, when required by the Authority, this column shall include any relevant amount related to CVA loss exposures arising from securities financing transactions.
19	**Advanced approach for CVA** Based on the relevant requirements specified in subregulation (19), this column shall reflect the relevant required risk weighted exposure amount for CVA risk, calculated in terms of the advanced approach, provided that, when required by the Authority, this column shall include any relevant amount related to CVA loss exposures arising from securities financing transactions.
20	**Total risk weighted exposure** This column shall reflect the relevant required aggregate amount of risk weighted exposure for counterparty credit risk, including any relevant amount of risk weighted exposure- (a) arising from OTC derivative instruments and securities financing transactions; (b) calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method; (c) related to CVA risk; (d) related to central counterparties.

Columns relating to counterparty credit risk analysis of standardised CVA risk weighted exposure: standardised approach, items 87 to 94

Column number	Description
2	**EAD** This column shall reflect the relevant exposure or EAD amount, calculated in terms of the relevant requirements specified in these Regulations, after the application of any relevant discount factor.
3	**Hedging: Single-name CDS** This column shall reflect the relevant required notional amount, after the application of any relevant discount factor, of a purchased single-name CDS, single-name contingent CDS and/or other eligible instrument used to hedge CVA risk.
4	**Hedging: Index CDS** This column shall reflect the relevant required notional amount, after the application of any relevant discount factor, of an eligible purchased index CDS used to hedge CVA risk.
5	**Standardised CVA risk weighted exposure** This column shall reflect the relevant required risk weighted exposure amount

	related to CVA risk, calculated in terms of the the relevant requirements specified in these Regulations for the standardised approach.

Columns relating to analysis of central counterparty trade exposure: standardised approach, items 95 to 98

Column number	Description
1	**Trade exposure** This column shall reflect the current and potential future exposure amount of a clearing member or a client to a central counterparty arising from any relevant OTC derivative instrument, exchange traded derivative transaction or securities financing transaction, calculated in accordance with the relevant requirements specified in subregulation (16) read with the relevant requirements respectively specified in subregulations (18) or (19) of these Regulations for the standardised approach or the internal model method.
3	**Risk weighted exposure** This column shall reflect the relevant required risk weighted exposure amount of a clearing member or a client to a central counterparty arising from any relevant OTC derivative instrument, exchange traded derivative transaction or securities financing transaction, calculated in accordance with the relevant requirements specified in subregulation (16) read with the relevant requirements respectively specified in subregulations (18) or (19) of these Regulations for the standardised approach or the internal model method.

Columns relating to analysis of qualifying central counterparty default fund guarantees: standardised approach, items 99 and 100

Column number	Description
1	**Initial margin collateral posted with a central counterparty** Based on the relevant requirements specified in these Regulations, this column shall reflect the relevant aggregate amount related to a clearing member's or client's funded collateral posted or provided to a central counterparty to mitigate the potential future exposure of the central counterparty to the clearing member arising from the possible future change in the value of their transactions, provided that, in accordance with the relevant requirements specified in these Regulations, initial margin shall exclude any relevant amount related to contributions to a central counterparty in terms of any mutualised loss sharing arrangement, that is, when a central counterparty uses initial margin to mutualise losses among the clearing members, the relevant amount shall be treated as a default fund exposure.
2	**Prefunded default fund contribution** This column shall reflect the relevant aggregate amount related to any prefunded default fund contributions made by the clearing member that will be applied upon such clearing member's default, either along with or immediately following such member's initial margin, to reduce any central counterparty loss.
3	**Trade exposure** This column shall reflect the relevant aggregate amount related to the current and potential future exposure of a clearing member or a client to a central counterparty arising from OTC derivatives, exchange traded derivatives transactions or securities financing transactions, calculated in accordance with the relevant requirements specified in these Regulations for the standardised approach or the internal model method.
4	**Risk weighted exposure** Based on the relevant requirements specified in subregulation (16), this column shall reflect the relevant calculated risk weighted exposure amount.

Columns relating to analysis of non-qualifying central counterparty default fund guarantees: standardised approach, items 101 and 102

Column number	Description
1	**Prefunded default fund contribution** This column shall reflect the relevant aggregate amount related to any prefunded default fund contribution by a clearing member that will be applied upon such clearing member's default, either along with or immediately

	following such member's initial margin, to reduce any central counterparty loss.
2	**Unfunded default fund contribution** This column shall reflect the relevant aggregate amount related to unfunded default fund contributions, which contributions- (a) are required to be paid by a clearing member when required by the relevant central counterparty; (b) will be applied upon such clearing member's default, either along with or immediately following such member's initial margin, to reduce any central counterparty loss.
4	**Risk weighted exposure** This column shall reflect the relevant aggregate risk weighted exposure amount equivalent to a deduction against capital and reserve funds.

Items relating to summary of selected credit risk related information: IRB approach

Item number	Description
108	**Impaired advances** This item shall reflect the relevant aggregate amount of advances in respect of which the bank raised a specific impairment. As a minimum, an advance is considered to be impaired when objective evidence exists that the bank is unlikely to collect the total amount due.
109 to 112	**Assets bought-in** These items shall reflect the relevant aggregate on-balance sheet carrying value of assets bought-in during the preceding five years to protect an investment, including a loan or advance, which assets have not been disposed of at the end of the reporting period.
113 to 115	**Credit impairments** These items shall reflect the relevant required aggregate amounts of specific credit impairments and portfolio credit impairments raised by the reporting bank in accordance with the relevant requirements specified in financial reporting standards issued from time to time.
117	**Total credit extended** This item shall reflect the relevant aggregate outstanding credit exposure amount due to the reporting bank in respect of loans, advances, off-balance-sheet exposure, derivative instruments and repurchase or resale agreements, before the effect of credit risk mitigation has been taken into consideration.
118	**Exposure at default (EAD)** This item shall reflect the reporting bank's relevant aggregate EAD amount, calculated in accordance with the relevant requirements specified in these Regulations.
119	**Average probability of default (PD, EAD weighted)** This item shall reflect the reporting bank's relevant EAD weighted average probability of default percentage, calculated in accordance with the relevant requirements specified in these Regulations.
120	**Average loss given default (LGD, EAD weighted)** This item shall reflect the reporting bank's relevant EAD weighted average LGD percentage relating to credit exposure, calculated in accordance with the relevant requirements specified in these Regulations.
121	**Total expected loss (EL)** Based on, amongst others, the relevant requirements specified in subregulation (21), this item shall reflect the reporting bank's relevant aggregate amount of expected loss.
122	**Best estimate of expected loss (BEEL)** Based on a PD of 100 per cent in respect of any relevant defaulted exposure, this item shall reflect the reporting bank's best estimate of expected loss

Item number	Description
	amount, which is expected to be an amount equal to or higher than the amount raised by the reporting bank in respect of specific credit impairment in accordance with the relevant requirements specified in financial reporting standards issued from time to time, provided that when the aforesaid two amounts differ the reporting bank shall at the written request of the Authority provide the Authority with a detailed reconciliation in writing between the two said amounts, which reconciliation shall duly explain the relevant reconciliation differences.

Columns relating to summary of on-balance-sheet and off-balance-sheet credit exposure: IRB approach, items 124 to 151

Column number	Description
1	**Utilised: on-balance-sheet exposure** This column shall reflect the relevant aggregate amount in respect of amounts drawn by clients, which amounts form part of the reporting bank's current on-balance-sheet exposure before the application of any credit risk mitigation (CRM).
2	**Off-balance-sheet exposure** This column shall reflect the relevant aggregate amount in respect of- (a) facilities granted to clients but not drawn, that is, unutilized facilities in respect of which no funds have been paid out and no debit balance has been raised; and (b) other off-balance-sheet items such as guarantees and commitments made by the reporting bank, which amounts form part of the reporting bank's total current exposure, before the application of any risk mitigation or relevant credit conversion factor.
3	**Repurchase and resale agreements** This column shall reflect the relevant aggregate amount in respect of any credit exposure arising from a repurchase or resale agreement concluded by the reporting bank.
4	**Derivative instruments** This column shall reflect the relevant aggregate amount in respect of any credit exposure arising from derivative instruments, including any relevant amount in respect of exposure to counterparty credit risk calculated in accordance with the relevant requirements specified in subregulations (15) to (19).
7	**Total credit exposure (EAD)** This column shall reflect the aggregate amount in respect of the reporting bank's relevant exposure weighted EAD amount, calculated in accordance with the relevant requirements specified in subregulations (11) and (13).
10	**Risk weighted exposure** This column shall include any relevant risk weighted exposure amount calculated in respect of the reporting bank's exposure to credit risk, after the application of a scaling factor of 1.06.
12	**Risk weighted exposure in respect of assets not subject to double default adjustment** This column shall reflect the relevant aggregate amount of credit exposure not subject to any double default adjustment as envisaged in subregulation (12)(g) or (14)(f).
13	**Risk weighted exposure in respect of assets subject to double default provisions, prior to adjustment** This column shall reflect the relevant aggregate amount of credit exposure subject to the requirements of double default envisaged in subregulation (12)(g) or (14)(f), prior to any relevant adjustment in respect of the said double default.

Columns relating to capital requirement in respect of specialised lending subject to specified risk

weights and specified risk grades: IRB approach, items 152 to 161

Column number	Description
1	**Credit exposure** This column shall reflect the relevant current exposure amount of the reporting bank in respect of any specialised lending subject to the risk weights and risk grades specified in subregulation (11)(d)(iii).
3	**Expected loss** This column shall reflect the relevant expected loss amount in respect of specialised lending, calculated in accordance with the relevant requirements specified in subregulation (21)(c).
4	**Specific credit impairment** This column shall reflect the relevant amounts in respect of specific credit impairment raised by the reporting bank in respect of specialised lending, calculated in accordance with the relevant requirements specified in financial reporting standards issued from time to time.
5	**Number of obligors** This column shall reflect the relevant number of obligors included in the specified risk weight category.

Items relating to reconciliation of credit impairments: IRB approach

Item number	Description
212	**Interest in suspense** Since interest income related to impaired loans may not ultimately contribute to income when doubt exists regarding the recovery of the relevant loan amount or related interest amount due, this item shall reflect the relevant amount of interest in suspense, that is, irrespective of the accounting treatment of interest income from time to time, this item shall reflect the difference between the relevant amount of interest contractually due to the reporting bank by its clients up to the end of the reporting month and the relevant amount of interest income actually included in the operating profit or loss of the bank.
215	**Recoveries** This item shall reflect the relevant aggregate amount in respect of recoveries, net of any relevant amount relating to specific credit impairment and/ or portfolio credit impairment.

Columns relating to analysis of past due exposure (EAD): IRB approach, items 219 to 246

Column number	Description
2, 4, 6 and 8	**Classified in default** Based on the respective EAD amounts and in respect of the relevant specified asset classes, these columns shall reflect an analysis of the relevant past due amounts classified as being in default, that is, due to matters such as, for example, early warning signs, an exposure may be classified as being in default even when the said exposure, for example, may not be legally overdue or overdue for more than 90 days.

Columns relating to counterparty credit risk: IRB approach, items 247 to 275

Column number	Description
1	**Replacement cost: OTC derivative instruments - unmargined transactions** In respect of unmargined transactions in OTC derivative instruments, this column shall reflect the relevant loss amount that would occur if a counterparty were to default and all relevant transactions were to be closed out immediately.
2	**Potential future exposure - add on: OTC derivative instruments: unmargined transactions** In respect of unmargined transactions in OTC derivative instruments, this column shall reflect the potential increase in exposure over a one-year time horizon from the relevant reporting date.

3	**Replacement cost: OTC derivative instruments - margined transactions** In respect of margined transactions in OTC derivative instruments, this column shall reflect the relevant loss amount that would occur if a counterparty were to default, assuming that the closeout and replacement of transactions occur instantaneously.
4	**Potential future exposure - add on: OTC derivative instruments: margined transactions** In respect of margined transactions in OTC derivative instruments, this column shall reflect the potential change in value of the relevant trades between the last exchange of collateral before default and replacement of the trades in the market, that is the margin period of risk.
5	**Credit exposure value** In the absence of an eligible master netting agreement, this column shall reflect the current value of all relevant credit exposures arising from securities financing transactions, after the effect of any relevant haircut has been taken into consideration.
6	**Collateral value** In the absence of an eligible master netting agreement, this column shall reflect the current value of eligible financial collateral obtained by the reporting bank in respect of all relevant securities financing transactions, after the effect of any relevant haircut has been taken into consideration.
7	**Netting benefit** This column shall reflect the aggregate amount of all relevant netting benefits arising from eligible master netting agreements taken into consideration in the calculation of the reporting bank's relevant adjusted credit exposure amount arising from securities financing transactions.
8	**Effective expected positive exposure** Based on the relevant requirements specified in subregulation (19)(a), this column shall reflect the relevant required effective expected positive exposure amount related to OTC derivative instruments.
9	**Stressed effective expected positive exposure** Based on the relevant requirements specified in, amongst others, subregulations (15) and (19) of these Regulations, this column shall reflect the relevant required effective expected positive exposure amount related to OTC derivative instruments in terms of a stressed scenario.
10	**Effective expected positive exposure** Based on the relevant requirements specified in subregulation (19)(a), this column shall reflect the relevant required effective expected positive exposure amount related to securities financing transactions.
11	**Stressed effective expected positive exposure** Based on the relevant requirements specified in, amongst others, subregulations (15) and (19) of these Regulations, this column shall reflect the relevant required effective expected positive exposure amount related to securities financing transactions in terms of a stressed scenario.
12	**Exposure amount: OTC derivative instruments – unmargined transactions** This column shall reflect the relevant required exposure or EAD amount in respect of unmargined transactions in OTC derivative instruments, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
13	**Exposure amount: OTC derivative instruments – margined transactions** This column shall reflect the relevant required exposure or EAD amount in respect of margined transactions in OTC derivative instruments, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
14	**Exposure amount - securities financing transactions**

	This column shall reflect the relevant required exposure or EAD amount for securities financing transactions, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
15	**Default risk - OTC derivative instruments – unmargined transactions** This column shall reflect the relevant required risk weighted exposure amount in respect of unmargined transactions in OTC derivative instruments, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
16	**Default risk - OTC derivative instruments – margined transactions** This column shall reflect the relevant required risk weighted exposure amount in respect of margined transactions in OTC derivative instruments, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
17	**Default risk - securities financing transactions** This column shall reflect the relevant required risk weighted exposure amount for securities financing transactions, calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method, which amount shall be net of any relevant incurred CVA loss amount.
18	**Standardised approach for CVA** Based on the relevant requirements specified in subregulation (15), this column shall reflect the relevant required risk weighted exposure amount for CVA risk, calculated in terms of the standardised approach, provided that, when required by the Authority, this column shall include any relevant amount related to CVA loss exposures arising from securities financing transactions.
19	**Advanced approach for CVA** Based on the relevant requirements specified in subregulation (19), this column shall reflect the relevant required risk weighted exposure amount for CVA risk, calculated in terms of the advanced approach, provided that, when required by the Authority, this column shall include any relevant amount related to CVA loss exposures arising from securities financing transactions.
20	**Total risk weighted exposure** This column shall reflect the relevant required aggregate amount of risk weighted exposure for counterparty credit risk, including any relevant amount of risk weighted exposure- (a) arising from OTC derivative instruments and securities financing transactions; (b) calculated in terms of the relevant requirements specified in these Regulations for the standardised approach or the internal model method; (c) related to CVA risk; (d) related to central counterparties.

Columns relating to counterparty credit risk analysis of standardised CVA risk weighted exposure: IRB approach, items 277 to 284

Column number	Description
2	**EAD** This column shall reflect the relevant exposure or EAD amount, calculated in terms of the relevant requirements specified in these Regulations, after the application of any relevant discount factor.
3	**Hedging: Single-name CDS** This column shall reflect the relevant required notional amount, after the application of any relevant discount factor, of a purchased single-name CDS, single-name contingent CDS and/or other eligible instrument used to hedge

	CVA risk.
4	**Hedging: Index CDS** This column shall reflect the relevant required notional amount, after the application of any relevant discount factor, of an eligible purchased index CDS used to hedge CVA risk.
5	**Standardised CVA risk weighted exposure** This column shall reflect the relevant required risk weighted exposure amount related to CVA risk, calculated in terms of the the relevant requirements specified in these Regulations for the standardised approach.

Columns relating to analysis of central counterparty trade exposure: IRB approach, items 285 to 288

Column number	Description
1	**Trade exposure** This column shall reflect the current and potential future exposure amount of a clearing member or a client to a central counterparty arising from any relevant OTC derivative instrument, exchange traded derivative transaction or securities financing transaction, calculated in accordance with the relevant requirements specified in subregulation (16) read with the relevant requirements respectively specified in subregulations (18) or (19) of these Regulations for the standardised approach or the internal model method.
3	**Risk weighted exposure** This column shall reflect the relevant required risk weighted exposure amount of a clearing member or a client to a central counterparty arising from any relevant OTC derivative instrument, exchange traded derivative transaction or securities financing transaction, calculated in accordance with the relevant requirements specified in subregulation (16) read with the relevant requirements respectively specified in subregulations (18) or (19) of these Regulations for the standardised approach or the internal model method.

Columns relating to analysis of qualifying central counterparty default fund guarantees: IRB approach, items 289 and 290

Column number	Description
1	**Initial margin collateral posted with a central counterparty** Based on the relevant requirements specified in these Regulations, this column shall reflect the relevant aggregate amount related to a clearing member's or client's funded collateral posted or provided to a central counterparty to mitigate the potential future exposure of the central counterparty to the clearing member arising from the possible future change in the value of their transactions, provided that, in accordance with the relevant requirements specified in these Regulations, initial margin shall exclude any relevant amount related to contributions to a central counterparty in terms of any mutualised loss sharing arrangement, that is, when a central counterparty uses initial margin to mutualise losses among the clearing members, the relevant amount shall be treated as a default fund exposure.
2	**Prefunded default fund contribution** This column shall reflect the relevant aggregate amount related to any prefunded default fund contributions made by the clearing member that will be applied upon such clearing member's default, either along with or immediately following such member's initial margin, to reduce any central counterparty loss.
3	**Trade exposure** This column shall reflect the relevant aggregate amount related to the current and potential future exposure of a clearing member or a client to a central counterparty arising from OTC derivatives, exchange traded derivatives transactions or securities financing transactions, calculated in accordance with the relevant requirements specified in these Regulations for the standardised approach or the internal model method.
4	**Risk weighted exposure** Based on the relevant requirements specified in subregulation (16), this column shall reflect the relevant calculated risk weighted exposure amount.

Columns relating to analysis of non-qualifying central counterparty default fund guarantees: IRB approach, items 291 and 292

Column number	Description
1	**Prefunded default fund contribution** This column shall reflect the relevant aggregate amount related to any prefunded default fund contribution by a clearing member that will be applied upon such clearing member's default, either along with or immediately following such member's initial margin, to reduce any central counterparty loss.
2	**Unfunded default fund contribution** This column shall reflect the relevant aggregate amount related to unfunded default fund contributions, which contributions- (a) are liable to be paid by a clearing member when required by the relevant central counterparty; (b) will be applied upon such clearing member's default, either along with or immediately following such member's initial margin, to reduce any central counterparty loss.
4	**Risk weighted exposure** This column shall reflect the relevant aggregate risk weighted exposure amount equivalent to a deduction against capital and reserve funds.

Columns relating to analysis of performing credit exposure, that is, EAD, analysed by effective maturity, items 308 to 320

Column number	Description
3 to 28	**EAD per specified asset class and effective maturity** Based on the relevant principles contained in, and the relevant requirements specified in, regulation 23(13)(d)(ii)(B), but disregarding any specified prudential floor or ceiling, these columns shall reflect the bank's performing credit exposure, that is, the relevant EAD amounts, according to the specified effective maturity bands.

".

Substitution of form BA 325

4. The form set out in Annexure B to this notice is hereby substituted for form BA 325 immediately preceding regulation 29 of the Regulations.

Substitution of form BA 340

5. The form set out in Annexure C to this notice is hereby substituted for Form BA 340 immediately preceding regulation 31 of the Regulations.

Amendment of regulation 31 of the Regulations

6. Regulation 31 of the Regulations is hereby amended:

(a) by the substitution in subregulation (3) for the heading and the words preceding paragraph (a) of the following heading and words:

"(3) *Criteria relating to categorisation of equity exposures held in a bank's banking book*

Based on the economic substance and not the legal form of an instrument, and irrespective of whether or not the said instrument makes provision for a voting right, for the purposes of these Regulations equity exposures held in a bank's banking book-";

(b) by the substitution in subregulation (6)(a) for subparagraph (xi) of the following subparagraph:

"(xi) the bank shall apply the relevant requirements specified in subregulation (7) below to any equity investment in any type of fund, held in the bank's banking book;

(c) by the substitution for subregulation (7) of the following subregulation:

"(7) *Matters related to the risk weighted exposure and related required amount of capital and reserve funds in*

respect of equity investments in all types of funds held in a bank's banking book

(a) Irrespective of whether a bank adopts the standardised approach or IRB approach for the measurement of the bank's exposure to credit risk, the bank shall use one of the alternative methodologies specified below for the calculation of its relevant risk weighted exposure amount in respect of its equity investments in all types of funds held in the bank's banking book, including any relevant off-balance-sheet exposure, such as, for example, an unfunded commitment to subscribe to a fund's future capital calls:

(i) when the bank is able to comply with the relevant specified conditions, the look-through approach specified in paragraph (b) below, which is the most granular approach;

(ii) when the bank is unable to comply with the relevant specified conditions related to the look-through approach, the mandate-based approach specified in paragraph (c) below, which provides an additional layer of risk sensitivity when compared to the look-through approach;

(iii) when neither of the aforementioned approaches is feasible, the fall-back approach specified in paragraph (d) below;

subject to the prior written approval of and such conditions as may be specified in writing by the Authority, a combination of the aforementioned three approaches, to determine the bank's capital requirement for an equity investment in an individual fund:

Provided that-

(A) the bank shall calculate its relevant risk weighted exposure amount in respect of any equity investment in all types of funds held in the bank's trading book in accordance with the relevant requirements specified in the form BA 320 read with regulation 28 of these Regulations;

(B) the bank may exclude from the look-through approach, mandate-based approach and the fall-back approach all equity investments in entities of which the debt obligations qualify for a risk weight of zero per cent in terms of the standardised approach for the measurement of the bank's exposure to credit risk, specified in regulation 23(8) of these Regulations;

(C) the bank shall exclude from the look-through approach, mandate-based approach and the fall-back approach any direct or indirect investment or exposure, including any relevant underlying exposure held by a fund, that is required to be deducted from the bank's capital and reserve funds in accordance with the relevant requirements specified in regulation 38(5) of these Regulations;

(D) when the bank has an investment in a fund, for example, Fund A, that itself has an investment in another fund, for example, Fund B, which the bank identified by using either the look-through approach or the mandate-based approach, the risk weight applied to the investment of the first fund, that is, Fund A's investment in Fund B, may be determined by using one of the three approaches set out above, provided that-

(i) for all subsequent layers, that is, for example, Fund B's investments in Fund C and so forth, the risk weights applied to the investment in Fund C may be determined in terms of the look-through approach only if the look-through approach was also used for determining the risk weight for the investment in the fund at the preceding layer, that is, the investment in Fund B;

(ii) when none of the aforementioned scenarios is applicable, the bank shall apply the fall-back approach in respect of the relevant investment in the fund;

(E) a bank that adopted the IRB approach for the measurement of the bank's exposure to credit risk-

(i) shall, in the case of the look-through approach, calculate the relevant IRB risk components, that is, the PD of the underlying exposures and, where applicable, the relevant LGD and EAD components, associated with the underlying exposures of the relevant fund, including, for example-

(aa) any underlying exposures arising from the fund's derivatives activities, when the underlying exposure has to be risk-weighted

in terms of the provisions of these Regulations; and

(bb) the associated counterparty credit risk exposure,

as if the bank was directly exposed to such risk, provided that, instead of determining a credit valuation adjustment (CVA) requirement associated with the fund's relevant derivatives exposures, the bank shall multiply the relevant exposure amount for counterparty credit risk with a factor of 1.5, before applying the risk weight associated with the relevant counterparty;

(ii) shall apply the relevant risk weights specified in the standardised approach in regulation 23(8) of these Regulations when an IRB calculation is not feasible, such as, for example, when the bank is unable to assign the necessary risk components to the relevant underlying exposures in a manner consistent with the bank's own underwriting criteria or the bank is using the mandate-based approach, provided that, in such cases, the bank shall-

(aa) in the case of equity exposures apply the simple risk weight method set out in subregulation (6)(b)(i) above;

(bb) in the case of securitisation exposures-

(i) apply the ratings-based approach set out in regulation 23(11)(e) of the Regulations or the Securitisation External Ratings-Based Approach (SEC-ERBA), whichever approach may be relevant from time to time; or

(ii) when directed in writing by the Authority or the bank is unable to use the SEC-ERBA, apply the Securitisation Standardised Approach (SEC-SA); or

(iii) apply a risk weight of 1250 per cent when the bank is unable to comply with the requirements specified for the use of the SEC-ERBA or SEC-SA; and

(cc) in all other cases, apply the standardised approach for credit risk;

(iii) may use the standardised approach for credit risk when applying risk weights to the underlying components of funds if the bank obtained the approval of the Authority to adopt the partial use approach in terms of the relevant provisions specified in regulation 36(3)(b)(i) of these Regulations in the case of directly held investments;

(iv) may, in the case of the look-through approach, rely on third-party calculations to determine the risk weights associated with the bank's equity investments in funds, that is, the risk weights related to the respective underlying exposures of the fund, if the bank does not have adequate data or information to perform the calculations itself, provided that, in such cases-

(aa) the third party shall use the respective methods related to the respective types of exposure specified in sub-item (ii) above; and

(bb) the bank shall apply a factor of 1.2 to the relevant risk weight that would otherwise apply if the exposure was held directly by the bank;

(b) Look-through approach (LTA)

When a bank is able to obtain sufficient and frequent information in respect of the underlying exposures of the relevant fund, and the said information is verified by a relevant independent third party, the bank shall adopt the look-through approach for the calculation of the bank's relevant risk weighted exposure amount in respect of its equity investments in all types of funds held in the bank's banking book, in terms of which approach the bank shall risk weight the fund's underlying exposures as if the exposures were held directly by the bank, provided that-

(i) the aforesaid requirement related to the frequency of financial reporting of the fund means that-

(A) the financial reporting of the fund is the same as or more frequently than the required reporting frequency of the bank; and

(B) the granularity of the relevant financial information is sufficient to calculate the relevant corresponding risk weights;

(ii) the aforesaid requirement related to the verification of the underlying exposures by a relevant independent third party-

(A) means that the relevant underlying exposures of the fund is verified, for example, by a depository or a custodian bank or, where applicable, the relevant management company; but does not mean or imply that any form of external audit is required in respect of the relevant underlying exposures;

(iii) the aforesaid requirement related to the risk weighting of the fund's underlying exposures includes, for example, any underlying exposure arising from the fund's derivatives activities, insofar as the relevant underlying exposure is otherwise required to be risk-weighted by a bank in terms of the provisions of these Regulations, and the associated counterparty credit risk exposure, as if the bank was directly exposed to such risk, provided that-

(A) instead of determining a credit valuation adjustment (CVA) requirement associated with the fund's relevant derivatives exposures, the bank shall multiply the relevant exposure amount for counterparty credit risk with a factor of 1.5, before applying the risk weight associated with the relevant counterparty;

(B) the aforesaid requirement to multiply the relevant exposure amount for counterparty credit risk with a factor of 1.5 shall not apply to situations in which the CVA capital requirement does not otherwise apply, such as, for example, transactions with a central counterparty or securities financing transactions (SFTs), unless the Authority determines in writing that the bank's CVA loss exposure arising from SFTs is material;

(iv) when the bank wishes to rely on third-party calculations in order to determine the relevant risk weights associated with the bank's equity investment in the fund, because the bank does not have adequate data or information to perform the required calculations itself, that is, the bank does not have adequate data or information itself to risk weight the relevant underlying exposures of the fund, the bank shall apply a factor of 1.2 to the applicable risk weight that would otherwise apply if the exposure was held directly by the bank.

For example, an exposure that is subject to a risk weight of 20 per cent in terms of the Standardised Approach shall be risk weighted at 24 per cent (1.2 * 20 per cent) when the bank wishes to rely on the look through performed by a third party;

(v) following the calculation of the aforesaid relevant total risk weighted exposure amount in respect of the fund, the bank shall calculate the average risk weight of the fund, denoted by Avg RWfund, by dividing the relevant total risk weighted exposure amount by the total assets of the fund;

(vi) following the calculation of the aforesaid relevant average risk weight of the fund the bank shall adjust upwards the average risk weight of the fund by its leverage, denoted by Lvg, for a given equity investment, through the application of the formula specified below:

$RWA_{investment}$ = Avg RWfund * Lvg * equity investment

Provided that the ultimate effective risk weight of the bank's investment in the fund, that is, Avg RWfund * Lvg, shall be subject to a limit of 1250 per cent.

(c) Mandate-based approach (MBA)

When a bank is unable to comply with the relevant requirements specified in paragraph (b) above in relation to the look-through approach, the bank may adopt the mandate-based approach for the calculation of the bank's relevant risk weighted exposure amount in respect of equity investments in all types of funds held in the bank's banking book, in terms of which approach the bank shall, as a minimum, use the information contained in a fund's mandate or in the relevant national regulations governing such investment funds, provided that-

(i) the aforesaid requirement to use the information contained in a fund's mandate or in the relevant national regulations governing such investment funds does not mean or imply that the bank is restricted to use only such information, and as such the bank may, for

example, also use information obtained from other relevant disclosures of the fund;

(ii) in order to ensure that all relevant underlying risks are duly accounted for, including any relevant exposure to counterparty credit risk, the relevant risk weighted exposure amount in respect of the fund shall be calculated as the sum of the items envisaged in items (A) to (C) below:

(A) in the case of any relevant balance sheet exposure, that is, in relation to the funds' assets, the bank shall risk weight the said assets assuming the underlying portfolios are invested to the maximum extent allowed in terms of the fund's mandate in those assets that are assigned the highest capital requirement, and then progressively in those other assets assigned lower capital requirements, provided that-

(i) when more than one risk weight may be applied to a given exposure, the bank shall apply the relevant highest risk weight.

For example, in the case of investments in corporate bonds with no ratings restrictions, the bank shall apply a risk weight of 150 per cent;

(B) when the underlying risk of a derivative exposure or an off-balance-sheet item is otherwise required to be risk weighted in terms of the provisions of these Regulations, the bank shall risk weight the relevant notional amount of the derivative position or of the off-balance sheet exposure accordingly, provided that-

(i) when the relevant underlying is unknown, the bank shall use the full notional amount of the relevant derivative positions for the calculation;

(ii) when the notional amount of the relevant derivative instrument is unknown, the bank shall conservatively estimate that amount, using the maximum notional amount of derivatives allowed under the relevant fund's mandate;

(C) in the case of any relevant exposure to counterparty credit risk associated with the fund's derivative exposures, the bank shall apply the standardised approach specified in regulation 23(18) of these Regulations for the measurement of the relevant exposure to counterparty credit risk, in terms of which approach the bank shall calculate the relevant amount of counterparty credit risk (CCR) exposure related to any relevant netting set of derivatives by multiplying the relevant sum of the replacement cost and potential future exposure with an alpha factor of 1.4, provided that-

(i) when the replacement cost is unknown, the bank shall conservatively calculate the relevant exposure measure for CCR by using the sum of the notional amounts of the relevant derivative instruments in the netting set as a proxy for the replacement cost, and the bank shall use a multiplier equal to 1 in the calculation of the relevant potential future exposure amount;

(ii) when the potential future exposure is unknown, the bank shall calculate the relevant exposure measure as 15% of the sum of the notional values of the relevant derivative instruments in the netting set, to reflect the potential future exposure amount;

(iii) when both the replacement cost and the add-on components are unknown, the bank shall calculate the relevant CCR exposure amount as:

1.4 * (sum of relevant notional amounts in the relevant netting set + 0.15*sum of relevant notional amounts in the relevant netting set);

(iv) the bank shall apply the relevant risk weight associated with the counterparty to the relevant sum of the aforesaid replacement cost and potential future exposure add-on;

(v) instead of determining a CVA requirement associated with the fund's derivative exposures in accordance with the relevant requirements specified in these Regulations, the bank shall multiply the relevant exposure amount to counterparty credit risk with a factor of 1.5, before applying the aforesaid risk weight associated with the relevant

counterparty, provided that the aforesaid requirement to multiply the relevant exposure amount for counterparty credit risk with a factor of 1.5 shall not apply to situations in which the CVA capital requirement does not otherwise apply, such as, for example, transactions with a central counterparty or securities financing transactions (SFTs), unless the Authority determines in writing that the bank's CVA loss exposure arising from SFTs is material;

(iii) following the calculation of the relevant risk weighted exposure amount in respect of the fund, as envisaged in subparagraph (ii) above, the bank shall calculate the average risk weight of the fund, denoted by Avg RWfund, by dividing the relevant total risk-weighted exposure amount by the total assets of the fund;

(iv) following the calculation of the aforesaid relevant average risk weight of the fund the bank shall adjust upwards the average risk weight of the fund by its leverage, denoted by Lvg, for a given equity investment, by multiplying the said average risk weight of the fund with the maximum financial leverage permitted in the fund's mandate or in the relevant national regulation governing the fund, through the application of the formula specified below:

$RWA_{investment}$ = Avg RWfund * Lvg * equity investment

Provided that the ultimate effective risk weight of the bank's investment in the fund, that is, Avg RWfund * Lvg, shall be subject to a limit of 1250 per cent;

(d) Fall-back approach (FBA)

When neither of the aforementioned two approaches is feasible for the bank, the bank shall apply to its relevant equity investment in the fund a risk weight of 1250 per cent.";

(d) by the deletion of the entire instruction relating to the completion of line item number 2 of form BA 340, specified in subregulation (8) (previously subregulation (7));

(e) by the substitution of the entire instruction relating to the completion of line item number 46, previously line item 43, of the BA 340, specified in the subregulation (8) (previously subregulation (7)), with the following instruction for the completion of line item number 46 of form BA 340:

"46 **Other investment in related entities**

This item shall reflect the aggregate amount of investments in subsidiaries and associates other than subsidiaries and associates reported in items 43 to 45, which subsidiaries and associates are included in the consolidation of the banking group's accounts.".

Amendment of regulation 36 of the Regulations

7. Regulation 36 of the Regulations is hereby amended:

(a) by the substitution in subregulation (3)(b) for subparagraph (i) of the following subparagraph:

"(i) the IRB approach for the measurement of a part of its relevant exposures to credit risk, the said bank or controlling company, as the case may be, shall, with the exception of its relevant exposure to central counterparties, as envisaged in regulation 23(16), adopt the said approach across all relevant significant asset classes, significant business units and relevant significant entities or activities within the banking group, provided that-";

(b) by the substitution in subregulation (3)(b)(i) for item (J) of the following item:

"(J) irrespective of materiality or significance, any relevant exposure to a central counterparty as envisaged in regulation 23(16), arising from an OTC derivative instrument, an exchange traded derivative instrument or a securities financing transaction, shall be treated in accordance with the relevant requirements specified in the said regulation 23(16), provided that, when assessing significance or materiality for purposes of item (D) above, the relevant measure or ratio shall be unaffected by the bank or controlling company's relevant exposure to central counterparties that are subject to the relevant requirements specified in regulation 23(16), that is, the said exposures shall be excluded from both the numerator and the denominator of any relevant ratio used for purposes of item (D) above;";

(c) by the substitution in subregulation (3)(b)(ii) for item (A) of the following item:

"(A) irrespective of the method adopted by the reporting bank or controlling company for the measurement of its exposure to counterparty credit risk arising from OTC derivative instruments or securities financing transactions, the bank or controlling company may adopt any of the methods envisaged in regulations

23(15) to 23(19) of these Regulations for the measurement of the bank or controlling company's consolidated exposure or EAD arising from long settlement transactions;";

(d) by the substitution in subregulation (3)(b)(ii) for item (B) of the following item:

"(B) in respect of exposure to counterparty credit risk for which the said bank or controlling company has not obtained approval from the Authority to adopt the internal model method, the bank or controlling company shall adopt within the banking group the standardised approach set out in regulation 23(18) for the measurement of the bank or controlling company's exposure to counterparty credit risk;";

(e) by the substitution in subregulation (4) for paragraph (b) of the following paragraph:

"(b) shall at the discretion of the relevant bank or controlling company, subject to the relevant requirements specified in subregulation (3), use one of the alternative methodologies specified below to determine its exposure to counterparty credit risk:

(i) The standardised approach specified in regulation 23(18);

(ii) Subject to the prior written approval of and such further conditions as may be specified in writing by the Authority, the internal model method specified in regulation 23(19);

(iii) Subject to the requirements specified in regulation 23(15), the prior written approval of and such further conditions as may be specified in writing by the Authority, a combination of the approaches specified in subparagraphs (i) and (ii) above;".

Substitution of form BA 610

8. The form set out in Annexure D to this notice is hereby substituted for form BA 610 immediately preceding regulation 37 of the Regulations.

Amendment of regulation 38 of the Regulations

9. Regulation 38 of the Regulations is hereby amended:

(a) by the substitution in subregulation (2) for paragraph (b) of the following paragraph:

"(b) shall at the discretion of the bank, use one of the alternative methodologies specified below to determine the bank's exposure to counterparty credit risk:

(i) the standardised approach specified in regulation 23(18);

(ii) subject to the prior written approval of and such further conditions as may be specified in writing by the Authority the internal model method specified in regulation 23(19);

(iii) subject to the relevant requirements specified in regulation 23(15) and the prior written approval of and such conditions as may be specified in writing by the Authority, a combination of the approaches envisaged in subparagraphs (i) and (ii) above;".

(b) by the substitution in subregulation (15)(e)(iv) for item (B) of the following item:

"(B) derivative exposures

A bank shall include in this category of derivative exposures the relevant amounts related to its exposures arising from the underlying of any relevant derivative contract, and the related counterparty credit risk (CCR) exposure amount, in accordance with such requirements as may be directed in writing by the Authority;".

Amendment of regulation 39 of the Regulations

10. Regulation 39 of the Regulations is hereby amended:

(a) by the substitution in subregulation (3) for paragraph (j) of the following paragraph:

"(j) interest-rate risk in the banking book;";

(b) by the substitution in subregulation (5) for paragraph (a) of the following paragraph:

"(a) shall be adequate for the size and nature of the activities of the bank, including, among others, the bank's-

(i) exposure to credit risk;

(ii) exposure to counterparty credit risk;

(iii) exposure to operational risk;

(iv) exposure to market risk;

(v) exposure to interest-rate risk in the banking book;

(vi) exposure to liquidity risk;

(vii) activities relating to risk mitigation;

(viii) trading activities,

and shall periodically be adjusted in light of the changing risk profile or financial strength of the bank, financial innovation or external market developments;";

(c) by the substitution in subregulation (5) for paragraph (c) of the following paragraph:

"(c) shall duly specify relevant limits and allocated capital relating to the bank's material exposures to risk;";

(d) by the insertion in subregulation (5)(d), of the following subparagraph after subparagraph (v):

"(vi) to ensure that the bank duly approves any significant hedging or risk management initiative, before it is implemented;";

(e) by the renumbering in subregulation (5)(d) of subparagraphs (vi) to (ix) as subparagraphs (vii) to (x), respectively;

(f) by the substitution in subregulation (5)(d), for the renumbered subparagraph (xi), previously subparagraph (x), of the following subparagraph:

"(xi) to ensure that, prior to its initiation, all relevant risk management, control and business units or lines appropriately review and assess proposed new activities, investment in new instruments or the introduction of new products, to ensure that the bank will be able to continuously understand, manage and control the relevant activity, investment or inherent risks in the product;";

(g) by the substitution in subregulation (5)(d), for the renumbered subparagraph (xv), previously subparagraph (xiv), of the following subparagraph:

"(xv) to enable the proactive identification and proper management of all relevant material exposures to risk;";

(h) by the substitution in subregulation (6)(b) for subparagraph (ii) of the following subparagraph:

"(ii) shall have sufficient expertise to understand the nature of the various instruments, markets and activities in which the bank conducts business, including capital market activities such as securitisation and the related off-balance sheet-activities, and the nature and extent of the associated risks;";

(i) by the substitution in subregulation (8)(n) for subparagraph (x) of the following subparagraph:

"(x) in respect of a measure or metric for which the bank obtained the prior written approval of the Authority to measure counterparty exposure, which measure shall be more conservative than the specified metric used to calculate EAD for every counterparty, that is, more conservative than alpha times Effective EPE, the bank shall regularly validate that the said measure or metric is sufficiently conservative;";

(j) by the substitution in subregulation (16) for the heading to paragraph (a) and the words in paragraph (a) preceding subparagraph (i) of the following heading and words:

"(a) Board and senior management oversight

Since sound governance and risk management processes provide the basis for ensuring, among other things, that a bank continuously maintains adequate capital and liquidity, the board of directors of a bank-
";

(k) by the insertion in subregulation (16)(a)(vii)(B) after sub-item (ii) of the following sub-item:

"(iii) shall in the case of the bank's exposure to interest-rate risk in the banking book comply with the relevant requirements specified in regulation 30 and such further requirements as may be specified in writing by the Authority;";

(l) by the renumbering in subregulation (16)(a)(vii)(B) of sub-items (iii) to (vi) as subitems (iv) to (vii), respectively;

(m) by the insertion in subregulation (16)(a)(vii) after item (B) of the following item:

"(C) develops a system to relate the bank's relevant-

(i) available amount of unencumbered level one and level two high-quality liquid assets to the bank's relevant expected total net cash outflows and/ or any related liquidity needs during a 30 calendar day time horizon under a significantly severe liquidity stress scenario, as envisaged in regulation 26(12);

(ii) available amount of stable funding to the bank's relevant required amount of stable funding, as envisaged in regulation 26(14),

that is, every bank shall have in place a robust internal liquidity adequacy assessment process (ILAAP), as part of the bank's overall risk management framework and processes;"; and

(n) by the renumbering in subregulation (16)(a)(vii) of items (C) to (F) as items (D) to (G), respectively.

Amendment of regulation 67 of the Regulations

11. Regulation 67 of the Regulations is hereby amended:

(a) by the insertion after the definition of "Basel III" of the following definition:

""**basis transaction"** in relation to the standardised approach for the measurement of a bank's exposure to counterparty credit risk means a non-foreign-exchange transaction, that is, both legs of the relevant transaction are denominated in the same currency, in respect of which the cash flows of both legs depend on different risk factors from the same asset class, which transactions may include, for example, interest rate basis swaps in respect of which payments based on two distinct floating interest rates are exchanged or commodity spread trades in respect of which payments based on prices of two related commodities are exchanged;".

(b) by the substitution for the definition of "hedging set" of the following definition:

"'**hedging set'** in relation to the standardised approach for the measurement of a bank's exposure to counterparty credit risk and the calculation of the add-on for each relevant asset class means a set of transactions within a single netting set within which partial or full offsetting is permitted for the purpose of calculating the relevant required potential future exposure add-on amount;";

(c) by the insertion after the definition of "hedging set" of the following definition:

"'**higher-level client'** in relation to the calculation of the relevant exposure to a central counterparty in a multi-level client structure means the institution that provides clearing services;";

(d) by the insertion after the definition of "lending related guarantee" of the following definition:

"'**leverage'** in relation to a bank's equity investments in all types of funds held in the bank's banking book means-

(a) the ratio of the relevant fund's total assets to its total equity; or

(b) such a more conservative ratio, calculated in such a manner, as may be specified in writing by the Authority;";

(e) by the insertion after the definition of "loss category" of the following definition:

"'**lower-level client'** in relation to the calculation of the relevant exposure to a central counterparty in a multi-level client structure means an institution that does clearing through a client that provides clearing services;";

(f) by the insertion after the definition of "mortgage loan or advance" of the following definition:

"'**multi-level client structure'** in relation to counterparty credit risk means a structure in terms of which a bank may centrally clear as an indirect client, that is, clearing services are provided to the bank by an institution or a person that is not a direct clearing member, but is itself a client of a clearing member or another clearing client, provided that for purposes of these Regulations, in relation to exposures between clients and clients of clients, the term "higher level client" and the term "lower level client" shall bear the meaning as defined hereinbefore;";

(g) by the substitution for the definition of "qualifying central counterparty" of the following definition:

"'**qualifying central counterparty'** means an entity or a person-

(a) that is-

(i) licensed to conduct business as a central counterparty, which license may include a license granted by way of a specific exemption;

(ii) permitted by the relevant regulator or supervisor to conduct business with or in respect of specified products and/or counterparties;

(iii) based in a jurisdiction in which it is prudentially supervised by a regulator or an authority that publicly confirms that all relevant central counterparties conducting business in that jurisdiction are continuously subject to rules and regulations that are in all material respects consistent with the relevant CPSS-IOSCO Principles for Financial Market Infrastructures, issued from time to time, provided that when a central counterparty conducts business in a jurisdiction that does not have a regulator or supervisor that applies the aforesaid Principles for Financial Market Infrastructures in respect of that central counterparty, the Authority may determine whether that central counterparty may be regarded as a qualifying central counterparty for purposes of these Regulations;

(b) that makes available to the relevant persons, such calculations, information or terms as may be specified or required in terms of the provisions of these Regulations to calculate the relevant required amount of capital and reserve funds for default fund exposures envisaged in regulation 23(16) of these Regulations; and

(c) that complies with such further requirements or criteria as may be specified in writing by the Authority or any other relevant regulator or supervisor from time to time;";

(h) by the insertion after the definition of "variation margin" of the following definition:

"'**volatility transaction**' in relation to the standardised approach for the measurement of a bank's exposure to counterparty credit risk means a transaction in terms of which the relevant reference asset depends on the historical or implied volatility of a relevant risk factor.".

12. **Date of commencement**

These Regulations shall come into operation on 1 January 2021.

CREDIT RISK **BA 200**
(Confidential and not available for inspection by the public) Monthly
Name of bank: .....
Month ended:.....(yyyy/mm/dd) Country:

(All amounts to be rounded off to the nearest R'000)

Standardised approach: Summary of selected credit risk related information	**Line no.**	**Total**
		1
Total gross loans and advances (item 24 of form BA100)	1	
Impaired advances[1]	2	
Assets bought-in (total of items 4 to 6)	3	
Immovable property (item 6, column 5, of form BA 220)	4	
Movable property	5	
Companies acquired (item 1, column 5, of form BA 220)	6	
Total credit impairments related to total gross loans and advances (item 25 of form BA 100)	7	
Total specific credit impairments (item 39, column 2, of form BA 200)	8	
Total portfolio credit impairments (item 39, column 3, of form BA 200)	9	
Credit losses charge to income statement (item 66 of form BA 120; item 45, column 1, of form BA 200)	10	
Total gross credit exposure (item 34, column 5, of form BA 200)	11	
Credit exposure post credit risk mitigation (item 34, column 14, of form BA 200)	12	
Credit exposure post credit risk mitigation and credit conversion factors (item 47, column 11, of form BA 200)	13	

1. **Means advances in respect of which the bank raised a specific impairment, and shall include any advance or restructured credit exposures subject to amended terms, conditions or concessions that are not formalised in writing.**

(All amounts to be rounded off to the nearest R'000)

Standardised approach: **Summary of on-balance sheet and off-balance sheet credit exposure**	**Line no.**	**On-balance sheet exposure**	**Off-balance sheet exposure**	**Repurchase and resale agreements[1]**	**Derivative instruments[2]**	**Total credit exposure pre CRM** (col. 1 to 4)	**Classification of total credit exposure[3] pre CRM**							
							Special mention[3]		**Sub-standard[3]**		**Doubtful[3]**		**Loss[3]**	
							Total	**of which: 60 < overdue days≤ 90**	**Total**	**of which: overdue > 90 days**	**Total**	**of which: overdue > 90 days**	**Total**	**of which: overdue > 90 days**
Asset class		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Corporate exposure (total of items 15 and 16)	14													
Corporate	15													
SME corporate	16													
Public sector entities	17													
Local government and municipalities	18													
Sovereign (including central government and central bank)	19													
Banks	20													
Securities firms	21													
Retail exposure (total of items 23, 24, 26 and 29)	22													
Residential mortgage advances	23													
Retail revolving credit[4]	24													
of which: credit cards	25													
SME retail (total of items 27 and 28)	26													
Secured lending	27													
Unsecured lending	28													
Retail – other	29													
of which: vehicle and asset finance	30													
unsecured lending[5, 6] ≤ R30 000	31													
unsecured lending[5] > R30 000	32													
Securitisation and resecuritisation exposure[7]	33													
Total (of items 14, 17 to 22 and 33)	34													

1. **Marked-to-market value.**
2. **In accordance with the relevant requirements specified in regulation 23.**
3. **In accordance with the relevant requirements specified in regulation 24(5).**
4. **As defined in regulation 23(11)(c)(iv)(B)(ii).**
5. **Relates to the relevant original exposure amount, excluding relevant retail revolving credit exposure and/or SME retail exposure.**
6. **Including loans in respect of which the maximum NCA rate applies.**
7. **Also refer to regulation 35 and the form BA500.**

(All amounts to be rounded off to the nearest R'000)

Standardised approach: **Summary of on-balance sheet and off-balance sheet credit exposure** **Asset class**	**Line no.**	**Credit exposure post CRM** **14**	**Specific credit impairment** **15**	**Total risk weighted exposure** **16**
Corporate exposure (total of items 15 and 16)	14			
Corporate	15			
SME corporate	16			
Public sector entities	17			
Local government and municipalities	18			
Sovereign (including central government and central bank)	19			
Banks	20			
Securities firms	21			
Retail exposure (total of items 23, 24, 26 and 29)	22			
Residential mortgage advances	23			
Retail revolving credit[4]	24			
of which: credit cards	25			
SME retail (total of items 27 and 28)	26			
Secured lending	27			
Unsecured lending	28			
Retail – other	29			
of which: vehicle and asset finance	30			
unsecured lending[5, 6] ≤ R30 000	31			
unsecured lending[5] > R30 000	32			
Securitisation and resecuritisation exposure[7]	33			
Total (of items 14, 17 to 22 and 33)	34			

1. **Marked-to-market value.**
2. **In accordance with the relevant requirements specified in regulation 23.**
3. **In accordance with the relevant requirements specified in regulation 24(5).**
4. **As defined in regulation 23(11)(c)(iv)(B)(ii).**
5. **Relates to the relevant original exposure amount, excluding relevant retail revolving credit exposure and/or SME retail exposure.**
6. **Including loans in respect of which the maximum NCA rate applies.**
7. **Also refer to regulation 35 and the form BA500.**

(All amounts to be rounded off to the nearest R'000)

Standardised approach: Reconciliation of credit impairments **Balance sheet**	**Line no.**	**Total credit impairments** (col 2 + col 3) **1**	**Specific credit impairments** **2**	**Portfolio credit impairments** **3**
Credit impairments: balance at beginning of period	35			
Income statement charge/ (reversal)	36			
Amounts written off against credit impairments	37			
Acquisition / disposal of subsidiaryand other	38			
Credit impairments: balance at end of period	39			
Memorandum item:				
Interest in suspense at end of period	40			

(All amounts to be rounded off to the nearest R'000)

Standardised approach: Reconciliation of credit impairments **Income statement**	**Line no.**	**Movement during reporting month** (col 2 + col 3) **1**	**Specific credit impairments** **2**	**Portfolio credit impairments** **3**
Credit impairments provision raised	41			
Credit impairments provision released	42			
Recoveries	43			
Suspended interest charge	44			
Total (of items 41 to 44)	45			
Memorandum item: Write offs not applied directly against the balance sheet, that is, provision not previously raised - when relevant	46			

(All amounts to be rounded off to the nearest R'000)

Standardised approach: Credit capital requirements **Based on risk weights**	**Line no.**	**Total gross credit exposure**[1]	**Specific credit impairment**	**Exposure amount post CRM and specific credit impairment**	**Breakdown of off-balance sheet exposure based on credit conversion factors (CCF)**							**Credit exposure value post CRM and CCF**	**Risk weighted exposure** (col. 11 *risk weight)
					0% ≤ CCF ≤ 5%	**5%< CCF ≤ 15%**	**15%< CCF ≤ 20%**	**20%< CCF ≤ 40%**	**50%**	**90%**	**100%**		
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Total (of items 48 to 53 and 56, 57, 60 and 63 to 67)	47												
0% risk weight	48												
10% risk weight	49												
20% risk weight	50												
35% risk weight	51												
40% risk weight	52												
50% risk weight	53												
of which[2]: *past due*	54												
without credit assessment by an eligible external credit assessment institution	55												
75% risk weight	56												
100% risk weight	57												
of which[2]: *past due*	58												
without credit assessment by an eligible external credit assessment institution	59												
150% risk weight	60												
of which[2]: *past due*	61												
without credit assessment by an eligible external credit assessment institution	62												
225% risk weight	63												
350% risk weight	64												
650% risk weight	65												
1250% risk weight	66												
Other prescribed risk weights	67												
of which[2]: *past due*	68												
without credit assessment by an eligible external credit assessment institution	69												

1. **Exposure value before the application of any credit conversion factor (CCF), credit risk mitigation (CRM) and any volatility adjustment.**
2. **When any exposure is both past due and unrated then the said exposure shall be included in BOTH categories.**

(All amounts to be rounded off to the nearest R'000)

Standardised approach: **Other assets**[1]	**Line no.**	**Amount**	**Specified risk weight (%)**	**Risk weighted exposure** (col. 1* col.2)
		1	**2**	**3**
Cash and balances with the central bank	70		0%	
Cash items in process of collection	71		20%	
Goodwill	72		Deduction[2]	
Intangibles other than goodwill	73		Deduction[2]	
Fixed assets (excl. assets bought-in)	74		100%	
Movable assets (excl. assets bought-in)	75		100%	
Assets bought-in	76		100%	
Lease residuals	77		100%	
Other assets	78		100%	
Total (of items 70 to 78)	79			

1. **Other assets are unrelated to credit risk but in order to calculate the reporting bank's relevant aggregate required amount of capital and reserve funds, for reconciliation to the form BA 700, such other assets are included in the form BA 200. When the majority of the reporting bank's credit exposure is subject to the IRB approach the bank shall complete the relevant required information specified in items 162 to 171 of the form BA 200 and leave open the relevant items under the standardised approach.**
2. **Relates to assets the relevant amounts of which are to be deducted from the reporting bank's capital and reserve funds in accordance with the relevant requirements specified in regulation 38(5).**

(All amounts to be rounded off to the nearest R'000)

Standardised approach: Analysis of counterparty credit risk exposure[1] Based on specified risk weights	Line no.	Standardised approach for counterparty credit risk						
		OTC derivative instruments				SFT[2]		
		Unmargined transactions		Margined transactions				
		Replacement cost	Potential future exposure add-on	Replacement cost	Potential future exposure add-on	Credit exposure value	Collateral value	Netting benefits
		1	2	3	4	5	6	7
Total (of items 81 to 85)	80							
0%	81							
20%	82							
50%	83							
100%	84							
150%	85							

1. Refer to regulations 23(15) to 23(19) for the relevant directives related to the measurement of a bank's exposure to counterparty credit risk.
2. Means Securities Financing Transactions. In accordance with the relevant requirements specified in regulation 23(15), a bank that did not obtain the approval of the AuthorityAuthority to adopt the Internal Model Method, shall calculate its exposure to credit risk arising from securities financing transactions in accordance with the relevant requirements specified in regulations 23(8) and 23(9).

(All amounts to be rounded off to the nearest R'000)

Standardised approach: Analysis of counterparty credit risk exposure[1] Based on specified risk weights	Line no.	Internal model[3]				Aggregate total across all relevant approaches								
		OTC derivative instruments		SFT[2]		Exposure amount			Risk weighted exposure					
									Default risk			CVA[4, 5] risk		Total risk weighted exposure
		Effective expected positive exposure	Stressed effective expected positive exposure	Effective expected positive exposure	Stressed effective expected positive exposure	OTC derivative instruments		SFT[2]	OTC derivative instruments		SFT[2]	Standardised	Advanced	
						Unmargined transactions	Margined transactions		Unmargined transactions	Margined transactions				
		8	9	10	11	12	13	14	15	16	17	18	19	20
Total (of items 81 to 85)	80													
0%	81													
20%	82													
50%	83													
100%	84													
150%	85													

1. Refer to regulations 23(15) to 23(19) for the relevant directives related to the measurement of a bank's exposure to counterparty credit risk.
2. Means Securities Financing Transactions. In accordance with the relevant requirements specified in regulation 23(15), a bank that did not obtain the approval of the Authority to adopt the Internal Model Method, shall calculate its exposure to credit risk arising from securities financing transactions in accordance with the relevant requirements specified in regulations 23(8) and 23(9).
3. In the case of cross-product netting, a bank shall report the relevant exposure under SFT.
4. Means credit valuation adjustment.
5. When the majority of the bank's credit exposure is subject to the IRB approach the bank shall complete the relevant required information specified in items 247 to 275 of the form BA 200, and leave open the relevant columns under the standardised approach.

Authority

Counterparty credit risk	Line no.	Alpha value
		1
Own estimate of alpha[1]	86	

1. Relates to internal model method only.

(All amounts to be rounded off to the nearest R'000)

Analysis of standardised CVA[1] risk weighted exposure	Line no	Weight	EAD	Hedging		Standardised CVA[1] risk weighted exposure[2]
				Single name CDS	Index CDS	
Ratings		1	2	3	4	5
AAA	87	0.70%				
AA	88	0.70%				
A	89	0.80%				
BBB	90	1.00%				
BB	91	2.00%				
B	92	3.00%				
CCC	93	10.00%				
Total (of items 87 to 93)	94					

1. Means credit valuation adjustment.
2. Total standardised CVA risk weighted exposure may not be equal to the sum of individual requirements calculated, due to, among other things, diversification benefits.

(All amounts to be rounded off to the nearest R'000)

Analysis of central counterparty trade exposure	Line no	Trade exposure	Risk weight	Risk weighted exposure	of which: calculated in terms of the standardised approach
		1	2	3	4
Exposures eligible for a 2% risk weight	95		2%		
Exposures eligible for a 4% risk weight	96		4%		
Exposures eligible for a bilateral risk weight	97				
Total central counterparty exposures (total of items 95 to 97)	98				

(All amounts to be rounded off to the nearest R'000)

Qualifying central counterparty default fund guarantees	Line no	Initial margin collateral posted with the CCP	Prefunded default fund contribution	Trade exposure	Risk weighted exposure
		1	2	3	4
Total	99				
(Specify)	100				

(All amounts to be rounded off to the nearest R'000)

Non-qualifying central counterparty default fund guarantees	Line no	Prefunded default fund contribution	Unfunded default fund contribution	Trade exposure	Risk weighted exposure
		1	2	3	4
Total	101				
(Specify)	102				

(All amounts to be rounded off to the nearest R'000)

Standardised approach: Residential mortgage exposure Analysed per specified loan-to-value (LTV) ratio[1, 2]	Line no.	Total exposure				*of which*: New business during the current reporting month			
		On-balance sheet exposure	Off-balance sheet exposure	Total gross credit exposure	Credit exposure value post CCF	On-balance sheet exposure	Off-balance sheet exposure	Total gross credit exposure	Credit exposure value post CCF
		1	2	3	4	5	6	7	8
Total (of items 104 to 106)	103								
LTV ratio ≤ 80%	104								
80% < LTV ratio <100%	105								
LTV ratio ≥ 100%	106								

1. Calculated based on the amount envisaged in regulation 23(6)(c).
2. An exposure shall be reported in only one of the relevant specified LTV-ratio buckets.

(All amounts to be rounded off to the nearest R'000[2])

IRB approach: Summary of selected credit risk related information	Line no.	Total 1
Total gross loans and advances (item 24 of form BA 100)	107	
Impaired advances[1]	108	
Assets bought-in (total of items 110 to 112)	109	
Immovable property (item 6, column 5, of form BA 220)	110	
Movable property	111	
Companies acquired (item 1, column 5, of form BA 220)	112	
Total credit impairments related to total gross loans and advances (item 25 of form BA 100)	113	
Total specific credit impairments (item 211, column 2, of form BA 200)	114	
Total portfolio credit impairments (item 211, column 3, of form BA 200)	115	
Credit losses charge to income statement (item 66, column 3, of form BA 120; item 217, column 1, of form BA 200)	116	
Total credit extended[2] (item 151, column 5, of form BA 200)	117	
Exposure at default (EAD) (item 151, column 7, of form BA 200)	118	
Average probability of default[3] (PD, EAD weighted) (item 200, column 3, of form BA 200)	119	
Average loss given default[3] (LGD, EAD weighted) (item 203, column 27, of form BA 200)	120	
Total expected loss (EL) (item 151, column 8)	121	
Best estimate of expected loss (BEEL)	122	
Net excess[4]/(deficit)[5] of total credit impairments compared to expected loss	123	

1. **Means advances in respect of which the bank raised a specific impairment, and shall include any advance or restructured credit exposures subject to amended terms, conditions or concessions that are not formalised in writing.**
2. **Not on an EAD basis.**
3. **Specified items require percentages instead of amounts to be reported, which percentages shall be rounded to two decimal places.**
4. **Refer to item 85 of form BA 700 and regulation 23(22)(d)(i)(B)(ii) when positive.**
5. **Refer to items 48 of form BA 700 and regulation 23(22)(d)(i)(B)(i) when negative.**

(All amounts to be rounded off to the nearest R'000)

IRB approach: Summary of on-balance sheet and off-balance sheet credit Asset class	Line no.	Utilised (On-balance-sheet exposure)	Off-balance-sheet exposure	Repurchase and resale agreements[1]	Derivative instruments[2]	Total credit extended[3] (col. 1 to 4)	*of which*: classified "in default"[4]	Total credit exposure (EAD)	Expected loss	Specific credit impairment	Total			
											Risk weighted exposure[5]	*of which*: attributed to defaulted assets	*of which*: not subject to double default adjustment	*of which*: subject to double default provisions prior to adjustment
		1	2	3	4	5	6	7	8	9	10	11	12	13
Corporate exposure (total of items 125 to 132)	124													
Corporate	125													
Specialised lending - high volatility commercial real estate (property development)	126													
Specialised lending - income producing real estate	127													
Specialised lending - object finance	128													
Specialised lending - commodities finance	129													
Specialised lending - project finance	130													
SME corporate	131													
Purchased receivables - corporate	132													
Public sector entities	133													
Local governments and municipalities	134													
Sovereign (including central government and central bank)	135													
Banks	136													
Securities firms	137													
Retail exposure (total of items 139, 140, 142, 145 and 149)	138													
Residential mortgage advances	139													
Retail revolving credit[6]	140													
of which: credit cards	141													
SME retail (total of items 143 and 144)	142													
Secured lending	143													
Unsecured lending	144													
Retail – other	145													
of which: vehicle and asset finance	146													
unsecured lending[7, 8] ≤ R30 000	147													
unsecured lending[7] > R30 000	148													
Purchased receivables - retail	149													
Securitisation and resecuritisation exposure[9]	150													
Total (of items 124, 133 to 138 and 150)	151													

1. **Marked-to-market value.**
2. **In accordance with the relevant requirements specified in regulation 23.**
3. **Not on an EAD basis.**
4. **Refer to the definition of default in regulation 67.**
5. **After the application of a scaling factor of 1.06.**
6. **As defined in regulation 23(11)(c)(iv)(B)(ii).**
7. **Relates to the relevant original exposure amount, excluding relevant retail revolving credit exposure and/or SME retail exposure.**
8. **Including loans in respect of which the maximum NCA rate applies.**
9. **Also refer to regulation 35 and the form BA500.**

(All amounts to be rounded off to the nearest R'000)

IRB approach: **Capital requirement i.r.o specialised lending subject to specified risk weights and specified risk grades**[1]	Line no.	Credit exposure	Risk weighted exposure[2] (col. 1* specified risk weight * scaling factor of 1.06)	Memorandum items:		
				Expected loss	Specific credit impairment	Number of obligors
		1	2	3	4	5
Specified risk weights						
0%	152					
50%	153					
70%	154					
90%	155					
95%	156					
115%	157					
120%	158					
140%	159					
250%	160					
Total (of items 152 to 160)	161					

1. **Should also be included in items 126 to 130.**
2. **After the application of a scaling factor of 1.06.**

(All amounts to be rounded off to the nearest R'000)

IRB approach: **Other assets**[1]	Line no.	Amount	Specified risk weight (%)	Risk weighted exposure (col. 1* col.2)
		1	2	3
Cash and balances with the central bank	162		0%	
Cash items in process of collection	163		20%	
Goodwill	164		Deduction[2]	
Intangibles other than goodwill	165		Deduction[2]	
Fixed assets (excl. assets bought-in)	166		100%	
Movable assets (excl. assets bought-in)	167		100%	
Assets bought-in	168		100%	
Lease residuals	169		100%	
Other assets	170		100%	
Total (of items 162 to 170)	171			

1. **Other assets are unrelated to credit risk but in order to calculate the reporting bank's relevant aggregate required amount of capital and reserve funds, for reconciliation to the form BA 700, such other assets are included in the form BA 200. When the majority of the reporting bank's credit exposure is subject to the standardised approach the bank shall complete the relevant required information specified in items 70 to 79 of the form BA 200 and leave open the relevant items under the IRB approach.**
2. **Relates to assets the relevant amounts of which are to be deducted from the reporting bank's capital and reserve funds in accordance with the relevant requirements specified in regulation 38(5).**

(All amounts to be rounded off to the nearest R'000)

IRB approach: Analysis of total credit exposure, that is, EAD, analysed by PD band Prescribed PD band	Line no.	Prescribed rating scale		Average PD of reporting bank[1] (%)	Asset class										
					Corporate exposure[2]									Public sector entities[2]	Local government and municipalities[2]
		Lower bound (%)	Upper bound (%)		Corporate	Specialised lending					SME corporate	Purchased receivables - corporate	Total corporate exposure (total of col. 4 to 11)		
						high volatility commercial real estate (property development)	income producing real estate	object finance	commodity finance	project finance					
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Performing (total of items 173 to 198)	172														
00	173		0.0000												
01	174	0.0001	0.0120												
02	175	0.0121	0.0170												
03	176	0.0171	0.0240												
04	177	0.0241	0.0340												
05	178	0.0341	0.0480												
06	179	0.0481	0.0670												
07	180	0.0671	0.0950												
08	181	0.0951	0.1350												
09	182	0.1351	0.1900												
10	183	0.1901	0.2690												
11	184	0.2691	0.3810												
12	185	0.3811	0.5380												
13	186	0.5381	0.7610												
14	187	0.7611	1.0760												
15	188	1.0761	1.5220												
16	189	1.5221	2.1530												
17	190	2.1531	3.0440												
18	191	3.0441	4.3050												
19	192	4.3051	6.0890												
20	193	6.0891	8.6110												
21	194	8.6111	12.1770												
22	195	12.1771	17.2220												
23	196	17.2221	24.3550												
24	197	24.3551	34.4430												
25	198	34.4431	99.9999												
Default	199	100.000	100.000												
Total (of items 172 and 199)	200														

1. Means the EAD weighted average probability of default (PD), calculated in accordance with the reporting bank's internal master rating scale and mapped to the relevant specified PD band.
2. In respect of the relevant specified PD bands and asset classes, a bank shall report the aggregate amount of its total credit exposure, that is, the relevant EAD amount, calculated in accordance with the relevant requirements specified in these Regulations.

(All amounts to be rounded off to the nearest R'000)

IRB approach: Analysis of total credit exposure, that is, EAD, analysed by PD band Prescribed PD band	Line no.	Asset class															Total credit exposure (EAD) (col. 12 to 18)
		Sovereign[1] (including central government and central banks)	Banks[1]	Securities firms[1]	Retail exposure[1]												
					Total retail exposure (total of columns 19 , 20, 22, 25 and 29)	Residential mortgage advances	Retail revolving credit		SME retail			Retail other				Purchased receivables retail	
							Total	of which: credit cards	Total (of col 23 and 24)	of which: secured lending	of which: unsecured lending	Total	of which: vehicle and asset finance	of which: unsecured lending ≤ R30 000	of which: unsecured lending > R30 000		
		15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Performing (total of items 173 to 198)	172																
00	173																
01	174																
02	175																
03	176																
04	177																
05	178																
06	179																
07	180																
08	181																
09	182																
10	183																
11	184																
12	185																
13	186																
14	187																
15	188																
16	189																
17	190																
18	191																
19	192																
20	193																
21	194																
22	195																
23	196																
24	197																
25	198																
Default	199																
Total (of items 172 and 199)	200																

1. In respect of the relevant specified PD bands and asset classes, a bank shall report the aggregate amount of its total credit exposure, that is, the relevant EAD amount, calculated in accordance with the relevant requirements specified in these Regulations.

IRB approach: EAD weighted average LGD (percentage)	Line no.	Asset class													
		Corporate exposure[1]													
		Corporate	Specialised lending					SME corporate	Purchased receivables - corporate	Total corporate exposure average LGD (%)	Public sector entities[1]	Local government and municipalities[1]	Sovereign[1] (including central government and central banks)	Banks[1]	Securities firms[1]
			high volatility commercial real estate (property development)	income producing real estate	object finance	commodity finance	project finance								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Performing	201														
Default	202														
Total average LGD	203														

1. In respect of the relevant specified asset classes, a bank shall report the EAD weighted average LGD percentage relating to the relevant credit exposure, calculated in accordance with the relevant requirements specified in these Regulations.

IRB approach: EAD weighted average LGD (percentage)	Line no.	Asset class												Total EAD weighted average LGD (%)
		Retail exposure[1]												
		Total retail exposure average LGD (%)	Residential mortgage advances	Retail revolving credit		SME retail			Retail other				Purchased receivables retail	
				Total	of which: credit cards	Total (of col 20 and 21)	of which: secured lending	of which: unsecured lending	Total	of which: vehicle and asset finance	of which: unsecured lending ≤ R30 000	of which: unsecured lending > R30 000		
		15	16	17	18	19	20	21	22	23	24	25	26	27
Performing	201													
Default	202													
Total average LGD	203													

1. In respect of the relevant specified asset classes, a bank shall report the EAD weighted average LGD percentage relating to the relevant credit exposure, calculated in accordance with the relevant requirements specified in these Regulations.

(All amounts to be rounded off to the nearest R'000)

IRB approach: Expected loss	Line no.	Asset class													
		Corporate exposure[1]													
		Corporate	Specialised lending					SME corporate	Purchased corporate receivables	Total corporate expected loss (total of col. 1 to 8)	Public sector entities[1]	Local government and municipalities[1]	Sovereign[1] (including central government and central banks)	Banks[1]	Securities firms[1]
			high volatility commercial real estate (property development)	income producing real estate	object finance	commodity finance	project finance								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Performing	204														
Default[2]	205														
Total expected loss (total of items 204 and 205)	206														

1. In respect of the relevant specified asset classes, based on the relevant requirements specified in these Regulations, a bank shall report its relevant aggregate expected loss amount.
2. Means the reporting bank's best estimate of the relevant expected loss amount.

(All amounts to be rounded off to the nearest R'000)

IRB approach: Expected loss	Line no.	Asset class												Total expected loss (total of col. 9 to 15)
		Retail exposure[1]												
		Total retail exposure expected loss (total of col 16, 17, 19, 22 and 26)	Residential mortgage advances	Retail revolving credit		SME retail			Retail other				Purchased retail receivables	
				Total	of which: credit cards	Total (of col 20 and 21)	of which: secured lending	of which: unsecured lending	Total	of which: vehicle and asset finance	of which: unsecured lending ≤ R30 000	of which: unsecured lending > R30 000		
		15	16	17	18	19	20	21	22	23	24	25	26	27
Performing	204													
Default[2]	205													
Total expected loss (total of items 204 and 205)	206													

1. In respect of the relevant specified asset classes, based on the relevant requirements specified in these Regulations, a bank shall report its relevant aggregate expected loss amount.
2. Means the reporting bank's best estimate of the relevant expected loss amount.

(All amounts to be rounded off to the nearest R'000)

IRB approach: **Reconciliation of credit impairments** **Balance sheet**	**Line no.**	**Balance sheet**		
		Total credit impairments (col. 2 + col. 3)	**Specific credit impairments**	**Portfolio credit impairments**
		1	**2**	**3**
Credit impairments: balance at beginning of period	207			
Income statement charge/ (reversal)	208			
Amounts written off against credit impairments	209			
Acquisition/disposal of subsidiary and other	210			
Credit impairments: balance at end of period	211			
Memorandum item:				
Interest in suspense at end of period	212			

IRB approach: **Reconciliation of credit impairments** **Income statement**	**Line no.**	**Income statement**		
		Movement during reporting month (col. 2 + col. 3)	**Specific credit impairments**	**Portfolio credit impairments**
		1	**2**	**3**
Credit impairments provision raised	213			
Credit impairments provision released	214			
Recoveries	215			
Suspended interest charge	216			
Total (of items 213 to 216)	217			
Memorandum item:				
Write offs not applied directly against the balance sheet, that is, provision not previously raised – when relevant	218			

(All amounts to be rounded off to the nearest R'000)

IRB approach: Analysis of past due exposure (EAD) Asset class	Line no.	Days overdue							
		1 - 30 days		31 - 60 days		61 - 90 days		>90 days	
		Total EAD		Total EAD		Total EAD		Total EAD	
			Of which: classified "in default[1]"		Of which: classified "in default[1]"		Of which: classified "in default[1]"		Of which: classified "in default[1]"
		1	2	3	4	5	6	7	8
Corporate exposure (total of items 220 to 227)	219								
Corporate	220								
Specialised lending - high volatility commercial real estate (property development)	221								
Specialised lending - income producing real estate	222								
Specialised lending - object finance	223								
Specialised lending - commodities finance	224								
Specialised lending - project finance	225								
SME corporate	226								
Purchased receivables - corporate	227								
Public sector entities	228								
Local government and municipalities	229								
Sovereign (including central government and central bank)	230								
Banks	231								
Securities firms	232								
Retail exposure (total of items 234, 235, 237, 240 and 244)	233								
Residential mortgage advances	234								
Retail revolving credit	235								
of which: credit cards	236								
SME retail (total of items 238 and 239)	237								
Secured lending	238								
Unsecured lending	239								
Retail – other	240								
of which: vehicle and asset finance	241								
unsecured lending ≤ R30 000 (see item 147 description)	242								
unsecured lending > R30 000 (see item 148 description)	243								
Purchased receivables - retail	244								
Securitisation and resecuritisation exposure	245								
Total credit exposure (EAD) (total of items 219, 228 to 233 and 245)	246								

1. Refer to definition of default specified in regulation 67.

(All amounts to be rounded off to the nearest R'000)

IRB approach: Analysis of counterparty credit risk exposure[1] Based on prescribed PD bands	Line no.	Standardised approach for counterparty credit risk						
		OTC derivative instruments				SFT[2]		
		Unmargined transactions		Margined transactions				
		Replacement cost	Potential future exposure add-on	Replacement cost	Potential future exposure add-on	Credit exposure value	Collateral value	Netting benefits
		1	2	3	4	5	6	7
Performing (total of items 248 to 273)	247							
00	248							
01	249							
02	250							
03	251							
04	252							
05	253							
06	254							
07	255							
08	256							
09	257							
10	258							
11	259							
12	260							
13	261							
14	262							
15	263							
16	264							
17	265							
18	266							
19	267							
20	268							
21	269							
22	270							
23	271							
24	272							
25	273							
Default	274							
Total counterparty credit risk (total of items 247 and 274)	275							

1. Refer to regulations 23(15) to 23(19) for the relevant directives related to the measurement of a bank's exposure to counterparty credit risk.
2. Means Securities Financing Transactions. In accordance with the relevant requirements specified in regulation 23(15), a bank that did not obtain the approval of the Authority to adopt the Internal Model Method, shall calculate its exposure to credit risk arising from securities financing transactions in accordance with the relevant requirements specified in regulations 23(8) and 23(9).

(All amounts to be rounded off to the nearest R'000)

IRB approach: Counterparty credit risk[1] Analysis of OTC derivative instruments and SFT[2] Based on prescribed PD bands	Line no.	Internal Model[3]				Aggregate total across all relevant approaches								
		OTC derivative instruments		SFT[2]		Exposure amount			Risk weighted exposure					
						OTC derivative instruments			Default risk[4]			CVA[5, 6] risk		
		Effective expected positive exposure	Stressed effective expected positive exposure	Effective expected positive exposure	Stressed effective expected positive exposure	Unmargined transactions	Margined transactions	SFT[2]	OTC derivative instruments		SFT[2]	Standardised	Advanced	Total risk weighted exposure
									Unmargined transactions	Margined transactions				
		8	9	10	11	12	13	14	15	16	17	18	19	20
Performing (total of items 248 to 273)	247													
00	248													
01	249													
02	250													
03	251													
04	252													
05	253													
06	254													
07	255													
08	256													
09	257													
10	258													
11	259													
12	260													
13	261													
14	262													
15	263													
16	264													
17	265													
18	266													
19	267													
20	268													
21	269													
22	270													
23	271													
24	272													
25	273													
Default	274													
Total counterparty credit risk (total of items 247 and 274)	275													

1. Refer to regulations 23(15) to 23(19) for the relevant directives related to the measurement of a bank's exposure to counterparty credit risk.
2. Means Securities Financing Transactions. In accordance with the relevant requirements specified in regulation 23(15), a bank that did not obtain the approval of the Authority to adopt the Internal Model Method, shall calculate its exposure to credit risk arising from securities financing transactions in accordance with the relevant requirements specified in regulations 23(8) and 23(9).
3. In the case of cross-product netting, a bank shall report the relevant exposure under SFT.
4. After the application of the scaling factor of 1.06.
5. Means credit valuation adjustment.
6. When the majority of the bank's credit exposure is subject to the standardised approach the bank shall complete the relevant required information specified in items 80 to 85 of the form BA 200 and leave open the relevant column under the IRB approach.

Authority**Counterparty credit risk**	Line no.	Alpha value
		1
Own estimate of alpha[1]	276	

1. **Relates to the internal model method only.**

(All amounts to be rounded off to the nearest R'000)

Analysis of standardised CVA[1] risk weighted exposure	Line no	Weight	EAD	Hedging		Standardised CVA[1] risk weighted exposure[2]
				Single name CDS	Index CDS	
Ratings		1	2	3	4	5
AAA	277	0.70%				
AA	278	0.70%				
A	279	0.80%				
BBB	280	1.00%				
BB	281	2.00%				
B	282	3.00%				
CCC	283	10.00%				
Total (of items 277 to 283)	284					

1. **Means credit valuation adjustment.**
2. **Total standardised CVA risk weighted exposure may not be equal to the sum of individual requirements calculated, due to, among other things, diversification benefits.**

(All amounts to be rounded off to the nearest R'000)

Analysis of central counterparty trade exposure	Line no	Trade exposure	Risk weight	Risk weighted exposure	of which: calculated in terms of the standardised approach
		1	2	3	4
Exposures eligible for a 2% risk weight	285		2%		
Exposures eligible for a 4% risk weight	286		4%		
Exposures eligible for a bilateral risk weight	287				
Total central counterparty exposures (total of items 285 to 287)	288				

(All amounts to be rounded off to the nearest R'000)

Qualifying central counterparty default fund guarantees	Line no	Initial margin collateral posted with the CCP	Prefunded default fund contribution	Trade exposure	Risk weighted exposure
		1	2	3	4
Total	289				
(Specify)	290				

(All amounts to be rounded off to the nearest R'000)

Non-qualifying central counterparty default fund guarantees	Line no	Prefunded default fund contribution	Unfunded default fund contribution	Trade exposure	Risk weighted exposure
		1	2	3	4
Total	291				
(Specify)	292				

(All amounts to be rounded off to the nearest R'000)

IRB approach: Residential mortgage exposure Analysed per specified loan-to-value (LTV) ratio[1, 2]	Line no.	Total exposure					*of which*: New business during the current reporting month				
		On-balance sheet exposure	Off-balance sheet exposure	Total gross credit exposure	EAD	Risk weighted exposure[3]	On-balance sheet exposure	Off-balance sheet exposure	Total gross credit exposure	EAD	Risk weighted exposure[3]
		1	2	3	4	5	6	7	8	9	10
Total (of items 294 to 296)	293										
LTV ratio ≤ 80%	294										
80% < LTV ratio <100%	295										
LTV ratio ≥ 100%	296										

1. Calculated based on the amount envisaged in regulation 23(6)(c).
2. An exposure shall be reported in only one of the relevant specified LTV-ratio buckets.
3. After the application of a scaling factor of 1.06.

(All amounts to be rounded off to the nearest R'000)

IRB approach: Analysis of total credit exposure, that is, EAD, analysed by LGD band Specified LGD band[1]	Line no.	Specified LGD band[1]		Asset class											
				Corporate exposure[1]											
					Specialised lending										
		Lower bound (%)	Upper bound (%)	Corporate	high volatility commercial real estate (property development)	income producing real estate	object finance	commodity finance	project finance	SME corporate	Purchased corporate receivables	Total corporate exposure (total of col. 3 to 10)	Public sector entities[1]	Local government and municipalities[1]	Sovereign[1] (including central government and central banks)
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
00	297		10.0000												
01	298	10.0001	20.0000												
02	299	20.0001	30.0000												
03	300	30.0001	40.0000												
04	301	40.0001	50.0000												
05	302	50.0001	60.0000												
06	303	60.0001	70.0000												
07	304	70.0001	80.0000												
08	305	80.0001	90.0000												
09	306	90.0001	100.0000												
10	307	100.0001	and more												

1. In respect of the relevant specified LGD bands and asset classes, a bank shall report the aggregate amount of its total credit exposure, that is, the relevant EAD amount, calculated in accordance with the relevant requirements specified in these Regulations.

(All amounts to be rounded off to the nearest R'000)

IRB approach: Analysis of total credit exposure, that is, EAD, analysed by LGD band Specified LGD band[1]	Line no.	Asset class														Total credit exposure (EAD) (total of col 11 to 17)
				Retail exposure[1]												
		Banks[1]	Securities firms[1]	Total retail exposure (total of col 18, 19, 21, 24 and 28)	Residential mortgage advances	Retail revolving credit		SME retail			Retail other				Purchased retail receivables	
						Total	of which: credit cards	Total (of col 22 and 23)	of which: secured lending	of which: unsecured lending	Total	of which: vehicle and asset finance	of which: unsecured lending ≤ R30 000	of which: unsecured lending > R30 000		
		15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
00	297															
01	298															
02	299															
03	300															
04	301															
05	302															
06	303															
07	304															
08	305															
09	306															
10	307															

1. In respect of the relevant specified LGD bands and asset classes, a bank shall report the aggregate amount of its total credit exposure, that is, the relevant EAD amount, calculated in accordance with the relevant requirements specified in these Regulations.

(All amounts to be rounded off to the nearest R'000)

Advanced IRB approach: Analysis of performing credit exposure, that is, EAD, analysed by effective maturity Specified maturity band[1]	Line no.	Specified maturity band[1]		Asset class[1]												
				Corporate exposure[3]												
					Specialised lending											
		Lower bound (years)[2]	Upper bound (years)[2]	Corporate	high volatility commercial real estate (property development)	income producing real estate	object finance	commodity finance	project finance	SME corporate	Purchased corporate receivables	Total corporate exposure (total of col. 3 to 10)	Public sector entities[3]	Local government and municipalities[3]	Sovereign[3] (including central government and central banks)
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
00	308		0.5000												
01	309	0.5001	1.0000												
02	310	1.0001	1.5000												
03	311	1.5001	2.0000												
04	312	2.0001	2.5000												
05	313	2.5001	3.0000												
06	314	3.0001	3.5000												
07	315	3.5001	4.0000												
08	316	4.0001	4.5000												
09	317	4.5001	5.0000												
10	318	5.0001	and longer												
Total EAD weighted average effective maturity - without the 1 year regulatory floor and the 5 year maximum[2]	319														
- with the 1 year regulatory floor and the 5 year maximum[4, 5]	320														

1. In respect of the relevant specified maturity bands and asset classes, a bank shall report the aggregate amount of its total credit exposure, that is, the relevant EAD amount, calculated in accordance with the relevant requirements specified in these Regulations, including the relevant principles contained in regulation 23(13)(d)(ii)(B).
2. The 1 year regulatory floor and the 5 year specified maximum effective maturity used for the calculation of minimum required capital and reserve funds shall be disregarded for purposes of the completion of line items 308 to 319.
3. Based on the same method used for the calculation of minimum required capital and reserve funds, such as the cash-flow formula or maximum remaining time, without taking into consideration the relevant specified 1 year regulatory floor and 5 year maximum effective maturity limit.
4. Means the EAD weighted effective maturity of the relevant asset class calculated in accordance with the relevant requirements specified in regulation 23(13)(d)(ii)(B), which average effective maturity shall be expressed in years and rounded to two decimal place.
5. The total EAD weighted effective maturity reported in column 29 shall include all relevant retail exposures.

(All amounts to be rounded off to the nearest R'000)

Advanced IRB approach: Analysis of performing credit exposure, that is, EAD, analysed by effective maturity Specified maturity band[1]	Line no.	Asset class[1]														Total credit exposure (EAD) (total of col 11 to 17)
		Banks[3]	Securities firms[3]	Retail exposure[4]												
				Total retail exposure (total of col 18, 19, 21, 24 and 28)	Residential mortgage advances	Retail revolving credit		SME retail			Retail other				Purchased retail receivables	
						Total	of which: credit cards	Total (of col 22 and 23)	of which: secured lending	of which: unsecured lending	Total	of which: vehicle and asset finance	of which: unsecured lending ≤ R30 000	of which: unsecured lending > R30 000		
		15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
00	308															
01	309															
02	310															
03	311															
04	312															
05	313															
06	314															
07	315															
08	316															
09	317															
10	318															
Total EAD weighted average effective maturity - without the 1 year regulatory floor and the 5 year maximum[2]	319															
- with the 1 year regulatory floor and the 5 year maximum[5, 6]	320															

1. In respect of the relevant specified maturity bands and asset classes, a bank shall report the aggregate amount of its total credit exposure, that is, the relevant EAD amount, calculated in accordance with the relevant requirements specified in these Regulations, including the relevant principles contained in regulation 23(13)(d)(ii)(B).
2. The 1 year regulatory floor and the 5 year specified maximum effective maturity used for the calculation of minimum required capital and reserve funds shall be disregarded for purposes of the completion of line items 308 to 319.
3. Based on the same method used for the calculation of minimum required capital and reserve funds, such as the cash-flow formula or maximum remaining time, without taking into consideration the relevant specified 1 year regulatory floor and 5 year maximum effective maturity limit.
4. Based on the maximum remaining time, without taking into consideration any relevant specified floor or maximum effective maturity limit.
5. Means the EAD weighted effective maturity of the relevant asset class calculated in accordance with the relevant requirements specified in regulation 23(13)(d)(ii)(B), which average effective maturity shall be expressed in years and rounded to two decimal place.
6. The total EAD weighted effective maturity reported in column 29 shall include all relevant retail exposures.

(All amounts to be rounded off to the nearest R'000)

IRB approach: Specified additional information	Line no.	Asset class												
		Corporate exposure									Public sector entities	Local government and municipalities	Sovereign (including central government and central banks)	Banks
		Corporate	Specialised lending					SME corporate	Purchased corporate receivables	Total corporate exposure (total of col.1 to 8)				
			high volatility commercial real estate (property development)	income producing real estate	object finance	commodity finance	project finance							
		1	2	3	4	5	6	7	8	9	10	11	12	13
EAD weighted average PD	321													
EAD weighted average PD excluding defaulted exposures	322													
Number[1] weighted average PD	323													
Number[1] weighted average PD excluding defaulted exposures	324													
EAD weighted average PD, excluding defaulted exposures,12 months ago	325													
Number[1] weighted average PD, excluding defaulted exposures,12 months ago	326													
Number[1] of performing counterparties[2] 12 months ago	327													
of which:														
Number[1] of defaulted counterparties[2] during the 12 months preceding the reporting month	328													
Number[1] of defaulted counterparties[2] during reporting month	329													
EAD of defaults during the reporting month	330													
Total number[1] of counterparties[2] in default at the end of the reporting month	331													

1. **The number of counterparties shall be based on the PD assignment level.**
2. **Multiple defaults on the same facility (retail exposure) or counterparty (non-retail exposure) shall be counted in the same way as in the PD estimation.**

(All amounts to be rounded off to the nearest R'000)

IRB approach: Specified additional information[1]	Line no.	Asset class													Total (of col 9 to 15)
		Securities firms	Retail exposure												
			Total retail exposure (total of col 16, 17, 19, 22 and 26)	Residential mortgage advances	Retail revolving credit		SME retail			Retail other				Purchased retail receivables	
					Total	of which: credit cards	Total (of col 20 and 21)	of which: secured lending	of which: unsecured lending	Total	of which: vehicle and asset finance	of which: unsecured lending ≤ R30 000	of which: unsecured lending > R30 000		
		14	15	16	17	18	19	20	21	22	23	24	25	26	27
EAD weighted average PD	321														
EAD weighted average PD excluding defaulted exposures	322														
Number[1] weighted average PD	323														
Number[1] weighted average PD excluding defaulted exposures	324														
EAD weighted average PD, excluding defaulted exposures,12 months ago	325														
Number[1] weighted average PD, excluding defaulted exposures,12 months ago	326														
Number[1] of performing counterparties[2] 12 months ago	327														
of which: Number[1] of defaulted counterparties[2] during the 12 months preceding the reporting month	328														
Number[1] of defaulted counterparties[2] during reporting month	329														
EAD of defaults during the reporting month	330														
Total number[1] of counterparties[2] in default at the end of the reporting month	331														
Hash total	332														

1. **The number of counterparties shall be based on the PD assignment level.**
2. **Multiple defaults on the same facility (retail exposure) or counterparty (non-retail exposure) shall be counted in the same way as in the PD estimation.**

DAILY REPORT: SELECTED RISK EXPOSURE **BA325**
(Confidential and not available for inspection by the public) Daily
Name of bank.....
Date.....(yyyy-mm-dd)

(All amounts to be rounded off to the nearest R'000)

Summary of selected information	Line no.	Total
		1
Market risk requirement (total of items 2 to 4)	1	
Minimum prescribed pillar 1 market risk requirement[1] (item 18, column 1, plus item 24, columns 1 to 4)	2	
Systemic risk add-on (pillar 2a) market risk requirement[2]	3	
Additionally specified bank-specific (pillar 2b) market risk requirement[3]	4	
Allocated capital and reserve funds for market risk	5	
Surplus/ (deficit) (item 5 less item 1)	6	
Memorandum items:		
Counterparty credit risk requirement (items 8 to 10)	7	
OTC	8	
SFT	9	
Credit-derivative instruments	10	
Liquidity risk		
SARB repo participation	11	
Liquid assets		
Held on preceding day	12	
Month to date average held	13	
Requirement (item 14 of form BA 310)	14	
Liquidity coverage ratio[4] (LCR)		
High quality liquid assets	15	
Net cash outflow	16	
LCR (item 15 divided by item 16, multiplied with 100)	17	

1. **Based on the minimum percentage requirement specified in item 9 column 3 of the form BA 700.**
2. **Based on the add-on percentage requirement specified in item 10 column 3 of the form BA 700.**
3. **Based on the add-on percentage requirement or amount reported in item 12 column 3 of the form BA 700.**
4. **Refer to regulation 26(12).**

(All amounts to be rounded off to the nearest R'000)

Standardised approach Position risk requirement	Line no.	Total	*of which:*	
			Specific risk	General risk
		1	2	3
Total (of items 19 to 23)	18			
Interest rate risk	19			
Equity risk	20			
Foreign exchange risk, including gold	21			
Commodity risk	22			
Options ("carved-out" positions)	23			

(All amounts to be rounded off to the nearest R'000)

Internal models approach Position risk requirement	Line no.	Regulatory VaR amounts[1, 2]			Incremental risk charge[1, 7]	Internal VaR[3]		Backtesting[4]	
		VaR[2]	VaR S (specific risk surcharge)	sVaR[2] (stressed VaR)		VaR amount	VaR limit	Hypothetical	Actual
		1	2	3	4	5	6	7	8
Total VaR amounts[5] and incremental risk amount	24								
Interest rate risk	25								
Equity risk	26								
Foreign exchange risk, including gold	27								
Commodity risk	28								
Other	29								
Diversification benefit	30								
Memorandum items:									
Total VaR amount[5, 6]	31								
Desk 1[6]	32								
Desk 2[6]	33								
Desk 3[6]	34								
Other desks[6]	35								

1. Calculated in accordance with the relevant requirements specified in these Regulations.

2. Based on, amongst other things, a 99 per cent, one-tailed confidence interval, and a minimum holding period of ten trading days.

3. May be based on a confidence interval and/or minimum holding period that differs from the requirements specified in these Regulations.

4. Number of exceptions recorded during the previous 250 days.

5. May not be equal to the sum of individual requirements calculated in respect of the respective risk categories or trading desks due to, amongst others, diversification benefits.

6. Please separately submit in writing the relevant desk description and other relevant information.

7. Refer to regulation 28(8)(h)(i)(E).

(All amounts to be rounded off to the nearest US $'000)

Foreign-currency exposure	Line no.	USD	Euro	GBP	CHF	JPY	Other	Total
		1	2	3	4	5	6	7
Total foreign-currency assets (net of infrastructural investments) (total of items 37 and 42)	36							
Non-residents (total of items 38 to 41)	37							
Foreign currency placed with non-residents	38							
Foreign currency placed in respect of securities borrowing	39							
Foreign currency on-lent to non-residents (line 40 equals line 55)	40							
Other foreign currency	41							
Residents (total of items 43 to 49)	42							
Customer foreign-currency accounts (CFC)	43							
Foreign currency placed in respect of securities borrowing	44							
Foreign currency placements with authorised dealers	45							
Foreign currency placements with S A Reserve Bank	46							
Foreign currency placed with residents, not specified above	47							
Gold coin and bullion	48							
Other foreign currency	49							
Total foreign-currency liabilities (total of items 51 and 56)	50							
Non-residents (total of items 52 to 55)	51							
Foreign-currency funding (loans received)	52							
Foreign-currency deposits attracted	53							
Foreign-currency deposits held in respect of securities lending	54							
Liability in respect of foreign-currency borrowings on-lent to non-residents	55							
Residents (total of items 57 to 60)	56							
Customer foreign-currency accounts (CFC)	57							
Foreign-currency accounts (CFA)	58							
Foreign-currency deposits held in respect of securities lending	59							
Foreign-currency placements from authorised dealers	60							
Commitments[1] to purchase foreign currency (total of items 62 and 67)	61							
Commitments[1] to purchase foreign currency against rand	62							
Residents	63							
Non-residents	64							
Authorised dealers	65							
S A Reserve Bank	66							
Commitments[1] to purchase foreign currency against foreign currency	67							
Commitments[1] to sell foreign currency (total of items 69 and 74)	68							
Commitments[1] to sell foreign currency against rand	69							
Residents	70							
Non-residents	71							
Authorised dealers	72							
S A Reserve Bank	73							
Commitments[1] to sell foreign currency against foreign currency	74							
Effective net open foreign-currency position(s) of reporting bank[1] (item 36 plus 61) less (50 plus 68) in each foreign currency and in all foreign currencies taken together	75							
Limit specified by the Registrar	76							
Internal overnight limits set by the bank's board of directors or senior management (in respect of each individual currency and in the aggregate)	77							

1. **Include all unsettled transactions, including spot, forward, options, futures and interest flows.**

(All amounts to be rounded off to the nearest R'000)

Summary of selected interbank information	Line no.	Overnight			Longer than overnight		
		Amount at the repo rate	Amount at other rates	Weighted average rate	Amount at the repo rate	Amount at other rates	Weighted average rate
		1	2	3	4	5	6
Total loans to or deposits with other domestic banks	78						
Specify (per institution)	79						
Total loans from or deposits by other domestic banks	80						
Specify (per institution)	81						
Hash total	82						

EQUITY RISK IN THE BANKING BOOK **BA 340**

(Confidential and not available for inspection by the public) Monthly

Name of bank……

Month ended……..(yyyy-mm-dd)

(All amounts to be rounded off to the nearest R'000)

Standardised approach for credit risk[1]	**Line no.**	**Exposure value**	**Risk weighting**	**Risk weighted exposure**	**Capital requirement**
		1	**2**	**3**	**4**
Equities - listed and unlisted	1		100%		
Equity specified in writing by the Authority	2		150%		

1. Including the simplified standardised approach for credit risk.

(All amounts to be rounded off to the nearest R'000)

IRB approach for credit risk **Market based approach**	**Line no.**	**Exposure value**	**Risk weighting**	**Risk weighted exposure**[1]	**Capital requirement**
		1	**2**	**3**	**4**
Simple risk weight method (total of items 4 and 5)	3				
Equities - listed	4		300%		
Equities - unlisted	5		400%		

		Exposure value	**Risk weighting floor**	**Risk weighted exposure**[1]		**Capital requirement**
				Without limit[2]	**With limit**[3]	
		1	**2**	**3**	**4**	**5**
Internal models approach (total of items 7 and 8)	6					
Equities - listed	7		200%			
Equities - unlisted	8		300%			
Memorandum item:						
Diversified amount	9					

1. **After the application of a scaling factor of 1.06.**
2. **Means the relevant risk weighted exposure amount prior to the application of the specified risk weighting floor, if relevant.**
3. **Means the relevant risk weighted exposure amount after the application of the specified risk weighting floor, when relevant.**

(All amounts to be rounded off to the nearest R'000)

IRB approach for credit risk PD/LGD approach Internal obligor grade[1]	Line no.	Internal rating: PD ratio			Exposure value		Risk weighted exposure[2]	Capital requirement
		PD range		Average PD assigned to the obligor grade (%)		In respect of which the 1,5 scaling factor applies		
		Lower bound (%)	Upper bound (%)					
		1	2	3	4	5	6	7
01	10	0.0001	0.0120					
02	11	0.0121	0.0170					
03	12	0.0171	0.0240					
04	13	0.0241	0.0340					
05	14	0.0341	0.0480					
06	15	0.0481	0.0670					
07	16	0.0671	0.0950					
08	17	0.0951	0.1350					
09	18	0.1351	0.1900					
10	19	0.1901	0.2690					
11	20	0.2691	0.3810					
12	21	0.3811	0.5380					
13	22	0.5381	0.7610					
14	23	0.7611	1.0760					
15	24	1.0761	1.5220					
16	25	1.5221	2.1530					
17	26	2.1531	3.0440					
18	27	3.0441	4.3050					
19	28	4.3051	6.0890					
20	29	6.0891	8.6110					
21	30	8.6111	12.1770					
22	31	12.1771	17.2220					
23	32	17.2221	24.3550					
24	33	24.3551	34.4430					
25	34	34.4431	99.9999					
Default	35	100.0000	100.0000					
Total (of items 10 to 35)	36							

1. **In ascending order, based on exposure weighted average PD.**
2. **After the application of a scaling factor of 1.06.**

(All amounts to be rounded off to the nearest R'000)

Equity investment in funds[1]	Line no.	Exposure value	Risk weighting	Risk weighted exposure	Capital requirement
		1	2	3	4
Look-through approach	37				
Mandate-based approach	38				
Fall-back approach	39		1250%		

1. **Relates to all banks, irrespective of whether the bank adopted the standardised approach or IRB approach for the measurement of the bank's exposure to credit risk.**

(All amounts to be rounded off to the nearest R'000)

Memorandum items:	Line no.	Exposure amount
		1
Equity exposures exempt from the market based and PD/LGD approaches	40	
Deductions against capital and reserve funds in respect of investments in related entities	41	
Investments in unconsolidated majority owned banking, securities and other financial subsidiaries	42	
Significant minority investments in banking, securities and other financial entities	43	
Investments in insurance subsidiaries and significant minority investments in insurance entities	44	
Significant minority and majority investments in commercial entities that exceed the specified materiality levels	45	
Other investments in related entities, which entities are included in the consolidation of the reporting banking group's accounts, such as significant minority- and majority-owned commercial entities below the specified materiality level	46	

FOREIGN OPERATIONS OF SOUTH AFRICAN BANKS **BA 610**
(Confidential and not available for inspection by the public) Quarterly
Name of entity..... Currency:.....
Quarter ended: ..... (yyyy-mm-dd) Country:.....
Host supervisor:.....
Rules applied[1]: .....

A. BALANCE SHEET (All amounts to be rounded off to the nearest '000)

Assets	Line no.	Banking	Trading	Total[2]
		1	2	3
Cash and balances with central bank	1			
Short term negotiable securities (total of items 3 to 5)	2			
Negotiable certificates of deposit	3			
Treasury bills	4			
Other	5			
Loans and advances to customers (item 7 less item 18)	6			
Gross loans and advances (total of items 8 to 17)	7			
Home loans	8			
Commercial Mortgages	9			
Credit cards	10			
Lease and instalment debtors	11			
Overdrafts	12			
Redeemable preference shares and other equivalent instruments	13			
Trade other bills and bankers acceptances	14			
Term loans	15			
Loans granted/ deposits placed under resale agreements	16			
Other loans to customers and clients	17			
Less: credit impairments	18			
Investment and trading securities (total of items 20 to 24, less item 25)	19			
Equities - Listed	20			
Equities - Unlisted	21			
Commodities	22			
Government and government - guaranteed securities	23			
Other dated securities	24			
Less: credit impairments	25			
Derivative financial instruments	26			
Pledged assets	27			
Investment in subsidiary companies	28			
Investments in associates and joint ventures	29			
Non-current assets held for sale	30			
Intangible assets	31			
Investment property	32			
Property and equipment	33			
Current income tax receivables	34			
Deferred income tax assets	35			
Post-employment assets	36			
Other assets	37			
TOTAL ASSETS (total of items 1, 2, 6, 19 and 26 to 37)	38			

1. **Reserve Bank, or host supervisor when the rules of a foreign supervisor were applied.**
2. **Actual balance at month-end.**

A. BALANCE SHEET (All amounts to be rounded off to the nearest '000)

Liabilities	Line no.	Banking	Trading	Total[1]
		1	2	3
Deposits, current accounts and other creditors (total of items 40 to 46)	39			
Current accounts	40			
Savings and deposits	41			
Call deposits	42			
Fixed and notice deposits	43			
Negotiable certificates of deposits	44			
Other deposits and loan accounts	45			
Deposits received under repurchase agreements	46			
Derivative financial instruments and other trading liabilities	47			
Term debt instruments (total of item 49 plus 50)	48			
Qualifying as capital	49			
Other	50			
Deferred revenue	51			
Current income tax liabilities	52			
Deferred income tax liabilities	53			
Non-current liabilities held for sale	54			
Retirement benefit obligations	55			
Provisions	56			
Other liabilities	57			
TOTAL LIABILITIES (total of items 39, 47, 48 and 51 to 57)	58			

Equity	Line no.	Banking	Trading	Total[1]
		1	2	3
Total equity attributable to equity holders (total of items 60 to 62)	59			
Share capital	60			
Retained earnings	61			
Other reserves	62			
Preference shareholders and minority shareholders equity (total of items 64 and 65)	63			
Minority interest	64			
Preference shareholders	65			
TOTAL EQUITY (total of items 59 and 63)	66			
TOTAL EQUITY AND LIABILITIES (total of items 58 and 66)	67			

Memorandum Items	Line no.	Banking	Trading	Total[1]
		1	2	3
Analysis of counterparties (item 6 - Loans and advances to customers)	68			
Loans and advances to non-bank customers	69			
Loans and advances to banks	70			
of which:				
Intra group	71			
Interbank	72			
Analysis of foreign currency (item 6 - Total foreign currency loans and advances included in item 6)	73			
Analysis of counterparties (item 39 - Deposits, current accounts and other creditors) (total of item 75 to 78, and 81 to 84)	74			
Sovereign, including central banks	75			
Public sector entities	76			
Local sector entities	77			
Banks (total of items 79 and 80)	78			
of which:				
Intra group	79			
Interbank	80			
Securities firms	81			
Corporate customers	82			
Retail customers	83			
Other	84			
Analysis of foreign currency (item 39) - Total foreign currency funding included in item 39	85			

1. **Actual balance at month-end.**

B. OFF BALANCE SHEET ACTIVITIES (All amounts to be rounded off to the nearest '000)

Description of item	Line no.	Banking	Trading	Total[1]
		1	2	3
Guarantees	86			
Letters of credit	87			
Customers' indebtedness for acceptances	88			
Committed undrawn facilities (including unutilised draw-down facilities)	89			
Underwriting exposures (including revolving underwriting exposures)	90			
Credit-derivative instruments	91			
Committed capital expenditure	92			
Operating lease commitments	93			
Other contingent liabilities	94			
of which: uncommitted undrawn facilities (including conditionally revocable undrawn loan commitments)	95			
TOTAL (of items 86 to 94)	96			

1. **Actual balance at month-end.**

C. INCOME STATEMENT (All amounts to be rounded off to the nearest '000)

Description of item	Line no.	Current quarter			Current year to date		
		Banking	Trading	Total[1]	Banking	Trading	Total[1]
		1	2	3	4	5	6
Interest and similar income (total of items 98, 99 and 110, less item 111)	97						
Short-term negotiable securities	98						
Loans and advances to customers (total of items 100 to 109)	99						
Homeloans	100						
Commercial mortgages	101						
Credit cards	102						
Lease instalment debtors	103						
Overdrafts	104						
Redeemable preference shares and other equivalent instruments issued to provide credit	105						
Trade, other bills and bankers acceptances	106						
Term loans	107						
Factoring accounts	108						
Other	109						
Government and other dated securities	110						
Less: interest income on trading assets allocated to trading revenue	111						
Interest expense and similar charges (total of items 113, 121 and 122, less item 123)	112						
Deposits, current accounts and other (total of items 114 to 116 and 119 to 120)	113						
Current accounts	114						
Savings and deposits	115						
Term and other deposits (total of items 117 and 118)	116						
Fixed and notice deposits	117						
Other	118						
Negotiable certificates of deposits	119						
Other deposits and loans	120						
Other liabilities	121						
Term debt instruments	122						
Less: interest expense on trading liabilities allocated to trading revenue	123						
Net interest income (item 97 less item 112)	124						

1. Actual balance at month-end.

C. INCOME STATEMENT (All amounts to be rounded off to the nearest '000)

Description of item	Line no.	Current quarter			Current year to date		
		Banking	Trading	Total[1]	Banking	Trading	Total[1]
		1	2	3	4	5	6
Net fee and commission income	125						
Dividend income	126						
Net trading income / (loss) (total of items 128 to 133)	127						
Foreign exchange	128						
Debt securities	129						
Commodities	130						
Derivative instruments	131						
Equities	132						
Other	133						
Other gains less losses	134						
Other operating income / (loss)	135						
Non interest revenue (total of items 125 to 127, 134 and 135)	136						
Gross operating income / (loss) (total of items 124 and 136)	137						
Credit losses	138						
Operating expenses (including indirect taxation) (total of items 140 to 148)	139						
Staff	140						
Computer processing	141						
Communication and travel	142						
Occupation and accommodation	143						
Marketing	144						
Fees and insurances	145						
Office equipment and consumables	146						
Auditors remuneration	147						
Other	148						
Operating profit/ (loss) before non-trading and capital items (total of item 137 less items 138 and 139)	149						
Non-trading and capital items	150						
Share of profit / (loss) of associates and joint ventures	151						
Profit / (loss) before income tax (total of items 149 to 151)	152						
Direct taxation	153						
Profit / (loss) for the period/ year (item 152 less item 153)	154						

1. Actual balance at month-end.

D1. CAPITAL ADEQUACY (All amounts to be rounded off to the nearest '000)

Summary information in respect of minimum required capital and reserve funds	Line no.	Risk exposure						
		Credit	Counterparty credit risk	Operational	Market	Equity	Other	Total
		1	2	3	4	5	6	7
Risk weighted exposure								
Risk weighted exposure equivalent amount prior to concentration risk	155							
Risk weighted exposure equivalent amount in respect of concentration risk	156							
Risk weighted exposure amount in respect of threshold items	157							
Aggregate risk weighted exposure equivalent amounts prior to specified add-ons or floors (total of item 155 to 157)	158							
Additional risk weighted exposure equivalent amounts specified by the Authority[1]	159							
Aggregate risk weighted exposure equivalent amounts (total of items 158 and 159)	160							
Aggregate risk weighted assets as reported in the most recently completed return submitted to the host supervisor	161							
Minimum required capital and reserve funds								
Base minimum required capital and reserve funds per specified risk type, based on risk-weighted exposure (item 160 multiplied with item 164, column 3)	162							
Minimum required capital and reserve funds, per specified risk type, based on risk-weighted exposure (item 160 multiplied with item 170, column 3)	163							

1. **Relates to items such as capital floors, add-ons to risk weighted exposure, etc.**

D2. CAPITAL ADEQUACY (All amounts to be rounded off to the nearest '000)

Summary information in respect of capital adequacy	Line no.	Percentages (Home)			Percentages (Host)[7]		
		Common equity tier 1 capital and reserve funds	Tier 1 capital and reserve funds	Total	Common equity tier 1 capital and reserve funds	Tier 1 capital and reserve funds	Total
		1	2	3	4	5	6
Base minima[1, 2]	164						
Add-on: idiosyncratic requirement specified by the Authority[3]	165						
Minimum required ratio, prior to buffers (total of items 164 and 165)	166						
Add-on: systemically important bank (SIB)[4]	167						
Add-on: countercyclical buffer[5]	168						
Add-on: conservation buffer[6]	169						
Total minimum required ratio (total of items 166 to 169)	170						
Capital adequacy ratio of the reporting bank	171						

1. **Includes pillar 2A.**
2. **Refer to regulations 38(8)(e)(i), 38(8)(e)(ii) and 38(9).**
3. **Refer to regulation 38(8)(e)(iii).**
4. **Refer to regulation 38(8)(e)(vi).**
5. **Refer to regulation 38(8)(e)(v) and 38(8)(g).**
6. **Refer to regulation 38(8)(e)(iv) and 38(8)(f).**
7. **Ratios, based on the rules of the relevant foreign/host supervisor. Non-Basel III entities to report total capital only.**

D3. CAPITAL ADEQUACY (All amounts to be rounded off to the nearest '000)

Minimum required capital and reserve funds	Line no.	'000 (Home)			'000 (Host)[3]		
		Common equity tier 1 capital and reserve funds	Tier 1 capital and reserve funds	Total	Common equity tier 1 capital and reserve funds	Tier 1 capital and reserve funds	Total
		1	2	3	4	5	6
Minimum required capital and reserve funds prior to specified floors or add-ons[1]	172						
Additional capital requirement specified by the home/host supervisor[2]	173						
Minimum required capital and reserve funds, including specified floors or add-ons (total of items 172 and 173)	174						
Aggregate amount of qualifying capital and reserve funds	175						
Excess / (shortfall) capital and reserve funds (item 175 minus item 174)	176						

1. **Home: item 160, column 7 multiplied by item 170, column 3. Host: item 161, column 7 multiplied by item 170, column 6.**
2. **To be specified by the Authority in writing.**
3. **Amounts, based on the rules of the relevant foreign/host supervisor. Non-Basel III entities to report total capital only.**

D4. CAPITAL ADEQUACY (All amounts to be rounded off to the nearest '000)

Qualifying capital and reserve funds	Line no.	Common equity tier 1 capital and reserve funds	Additional tier 1 capital and reserve funds	Tier 2 capital and reserve funds	Total (sum of col 1 to 3)
		1	2	3	4
Paid in capital and qualifying instruments	177				
Retained earnings	178				
Accumulated other comprehensive income (and other reserves)[1]	179				
Regulatory adjustments	180				
Aggregate amount of qualifying capital and reserve funds	181				

1. **General allowance for credit impairments and excess amount of provisions over expected losses to be included in column 3.**

E. 1 CREDIT RISK (All amounts to be rounded off to the nearest '000)

Standardised approach: Summary of credit exposure and risk weighted exposure	Line no.	**Credit risk exposure**[1]							**Credit impairment related information**		**Credit risk classification**			
		On-balance sheet exposure	**Off-balance sheet exposure**	**Repurchase and Resale agreements**	**Derivative instruments**	**Total credit exposure** (total of col. 1 to 4)	**Total credit exposure post CRM**	**Risk weighted exposure**	**Impaired advances**	**Specific credit impairment**	**Special mention**	**Sub-standard**	**Doubtful**	**Loss**
Based on asset class		1	2	3	4	5	6	7	8	9	10	11	12	13
Corporate exposure (total of items 183 and 184)	182													
Corporate	183													
SME corporate	184													
Public sector entities	185													
Local governments and municipalities	186													
Sovereign (including central government and central bank)	187													
Banks	188													
Securities firms	189													
Retail exposure (total of items 191 to 194)	190													
Residential mortgages (including any home equity line of credit)	191													
Retail revolving credit	192													
Retail - other	193													
SME retail	194													
Other assets	195													
Securitisation and resecuritisation exposure	196													
Total (of items 182, 185 to 190, 195 and 196)	197													

1. **Including all relevant amounts reported in item 231.**

E. 2 CREDIT RISK (All amounts to be rounded off to the nearest '000)

Standardised and/or IRB approach: Credit concentration risk: large exposure to a person[1] Name of person	Line no.	Asset class[2]	Total credit exposure[3]: exposures exceeding 10% of qualifying capital and reserve funds per person	Total credit exposure[3]: exposures exceeding 25% of qualifying capital and reserve funds per person	Credit risk mitigation	Risk weighted value[4] of net exposure
		1	2	3	4	5
Private-sector non bank: total	198					
(Specify)	199					
	200					
	201					
Bank/regulated securities firm: total	202					
(Specify)	203					
	204					
	205					
Other: total	206					
Specify)	207					
	208					
	209					
	210					
Total (of items 198, 202 and 206)	211					

1. Refer to section 73 of the Act and regulations 24(6) to 24(8).
2. Based on the following specified keys: 1 = Corporate; 2 = SME corporate; 3 = Public sector entities; 4 = Local government and municipalities; 5 = Sovereign (including central governments and central bank); 6 = Banks; 7 = Securities firms; 8 = Retail; 9 = SME retail 10 = Securitisation or resecuritisation exposure
3. Before the application of any credit conversion factor, credit risk mitigation or volatility adjustment.
4. After the application of a scaling factor of 1.06 in the case of the IRB approach.

E.3 CREDIT RISK (All amounts to be rounded off to the nearest '000)

IRB approach : **Summary of credit exposure and risk weighted exposure** **Based on asset class**	**Line no.**	**Credit Risk Exposure[1]**											**Credit impairments**	
		On-balance sheet exposure	**Off-balance sheet exposure**	**Repurchase and resale agreements**	**Derivative instruments**	**Total credit extended[2]** (col. 1 to 4)	**Total credit exposure (EAD)**	***of which*: Defaulted EAD**	**Average PD %**	**Average LGD %**	**Risk weighted exposure[3]**	**Expected loss**	**Impaired advances**	**Specific credit Impairments**
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Corporate exposure (total of items 213 to 216)	212													
Corporate	213													
Specialised lending	214													
SME corporate	215													
Purchased receivables - corporate	216													
Public sector entities	217													
Local governments and municipalities	218													
Sovereign (including central government and central bank)	219													
Banks	220													
Securities firms	221													
Retail exposure (total of items 223 to 227)	222													
Residential mortgages (including any home equity line of credit)	223													
Retail revolving credit	224													
Retail - other	225													
SME retail	226													
Purchased receivables - retail	227													
Other assets	228													
Securitisation and resecuritisation exposure	229													
Total (of items 212, 217 to 222, 228 and 229)	230													

1. **Including all relevant amounts reported in item 231.**
2. **Not on a EAD basis.**
3. **After the application of a scaling factor of 1.06.**

E.4 CREDIT RISK (All amounts to be rounded off to the nearest '000)

Standardised / IRB approach: Counterparty credit risk[1] Analysis of OTC derivative instruments and SFT[2] Based on specified risk weights	Line no.	Aggregate total across all relevant approaches										
		Exposure amount[1]			Risk weighted exposure							
		OTC derivative instruments		SFT[2]	Default risk[3]		CVA[4] risk		Central counterparty trade exposure	Qualifying central counterparty default fund	Non-qualifying central counterparty default fund	Total
		Unmargined transactions	Margined transactions		OTC derivative instruments	SFT[2]	Standardised	Advanced				
		1	2	3	4	5	6	7	8	9	10	11
Total	231											

1. Refer to regulations 23(15) to 23(19) for the relevant directives related to the measurement of a bank's exposure to counterparty credit risk.
2. Means Securities Financing Transactions. In accordance with the relevant requirements specified in regulation 23(15), a bank that did not obtain the approval of the Authority to adopt the Internal Model Method, shall calculate its exposure to credit risk arising from securities financing transactions in accordance with the relevant requirements specified in regulations 23(8) and 23(9).
3. After the application of a scaling factor of 1.06 in the case of the IRB approach.
4. Means credit valuation adjustment.

F1. LIQUIDITY RISK[1] (All amounts to be rounded off to the nearest '000)

Description of item	Line no.	Total	Next day	2 days to 1 month	More than 1 month to 2 months	More than 2 months to 3 months	More than 3 months	Non contractual
		1	2	3	4	5	6	7
Contractual exposure:								
Contractual maturity of assets	232							
Contractual maturity of liabilities	233							
On-balance sheet contractual mismatch (item 232 less item 233)	234							
Cumulative on-balance sheet contractual mismatch	235							
Contractual off-balance-sheet exposure	236							
BaU exposure:								
BaU[1] maturity of assets	237							
BaU[1] maturity of liabilities	238							
On-balance sheet BaU mismatch (item 237 less item 238)	239							
Cumulative on-balance sheet BaU mismatch	240							
BaU off-balance-sheet exposure	241							
Stressed exposure:								
Stressed[1] maturity of assets	242							
Stressed[1] maturity of liabilities	243							
On-balance sheet stress mismatch (item 242 less item 243)	244							
Cumulative on-balance sheet stress mismatch	245							
Stressed outflows arising from off-balance-sheet exposure	246							
Total available stress funding	247							
Funding received from 10 largest depositors	248							

1. Refer to regulation 26 and the form BA300 for the relevant detailed directives.

F2. LIQUIDITY RISK (All amounts to be rounded off to the nearest '000)

Liquidity coverage ratio[1] (LCR)	Line no.	Home		Host	
		Total	Weighted total	Total	Weighted total
		1	2	3	4
Total qualifying high-quality liquid assets (total of items 250 to 252)	249				
Level one high-quality liquid assets	250				
Level two high-quality liquid assets	251				
Other qualifying assets/facilities[2] Please specify	252				
Total outflows (total of items 254 to 257)	253				
Retail deposits	254				
Unsecured wholesale funding	255				
Secured funding	256				
Other expected outflows	257				
Total inflows (total of items 259 to 263)	258				
Maturing secured lending transactions	259				
Net inflows from retail and small business	260				
Net inflows from wholesale non-financial institutions	261				
Net inflows from financial institutions and central banks	262				
Other cash inflows	263				
Total net cash outflows (item 253 minus min[item 258, 75% of item 253])	264				
Liquidity coverage ratio (item 249 divided by item 264, multiplied with 100)	265				

1. **Refer to regulation 26(12) for the relevant detailed directives.**
2. **Relates to Alternative Liquidity Approaches as outlined in paragraphs 55 to 67 of Basel III: The Liquidity Coverage Ratio and liquidity risk monitoring tools (January 2013).**

G. MARKET RISK (All amounts to be rounded off to the nearest '000)

Description of item	Line no.	Standardised approach			Internal models approach[1]				Total (of col. 1 to 7)
		General risk	Specific risk	Options	VaR	sVaR	Specific risk add-on	Incremental risk charge[1]	
		1	2	3	4	5	6	7	8
Interest rate risk	266								
Equity position risk	267								
Foreign exchange risk	268								
Commodities risk	269								
Other	270								
Total (of items 266 to 270)	271								
Risk-weighted exposure equivalent amount (item 271 multiplied by 12.5)[2]	272								

1. **Calculated in accordance with the relevant requirements specified in regulation 28(8) read with the relevant requirements specified in this regulation 37.**
2. **Based on the higher of the relevant home or host capital requirement.**

H. INTEREST-RATE RISK: BANKING BOOK (All amounts to be rounded off to the nearest '000)

Static repricing gap	Line no.	Up to 1 month	More than 1 month to 3 months	More than 3 months to 6 months	More than 6 months to 12 months	More than 12 months to 3 years	More than 3 years to 5 years	More than 5 years to 10 years	More than 10 years	Non-rate sensitive items	Total
		1	2	3	4	5	6	7	8	9	10
Assets[1]	273										
Liabilities[1] and capital and reserve funds	274										
Net static gap excluding derivative instruments (item 273 minus item 274)	275										
Net static gap, including derivative instruments	276										

1. **Excluding derivative instruments.**

I. EQUITY RISK IN THE BANKING BOOK (All amounts to be rounded off to the nearest '000)

Standardised approach for credit risk[1]	Line no.	Exposure value	Risk weighting	Risk weighted exposure	Capital requirement
		1	2	3	4
Equities - listed and unlisted	277		100%		
Equity specified in writing by the Authority	278		150%		

1. **Including the simplified standardised approach for credit risk.**

(All amounts to be rounded off to the nearest '000)

IRB approach for credit risk Market based approach	Line no.	Exposure value	Risk weighting	Risk weighted exposure[1]	Capital requirement
		1	2	3	4
Simple risk weight method (total of items 280 and 281)	279				
Equities - listed	280		300%		
Equities - unlisted	281		400%		

IRB approach for credit risk Internal models approach		Exposure value	Risk weighting floor	Risk weighted exposure[1]		Capital requirement
				Without limit[2]	With limit[3]	
		1	2	3	4	5
Internal models approach (total of items 283 and 284)	282					
Equities - listed	283		200%			
Equities - unlisted	284		300%			
Memorandum item:						
Diversified amount	285					

1. **After the application of a scaling factor of 1.06.**
2. **Means the relevant risk weighted exposure amount prior to the application of the specified risk weighting floor, if relevant.**
3. **Means the relevant risk weighted exposure amount after the application of the specified risk weighting floor, when relevant.**

CONTINUES ON PAGE 258 - PART 3

Vol. 666 31 December Desember 2020 No. 44048

PART 3 OF 3

(All amounts to be rounded off to the nearest '000)

IRB approach for credit risk PD/LGD approach	Line no.	Exposure value		Average risk weighted exposure[1]	Capital requirement
		Total	In respect of which the 1,5 scaling factor applies		
		1	2	3	4
Total (of items 287 and 288)	286				
Total of performing categories	287				
Total of default categories	288				

1. After the application of a scaling factor of 1.06.

(All amounts to be rounded off to the nearest R'000)

Equity investment in funds[1]	Line no.	Exposure value	Risk weighting	Risk weighted exposure	Capital requirement
		1	2	3	4
Look-through approach	289				
Mandate-based approach	290				
Fall-back approach	291		1250%		

1. Relates to all banks, irrespective of whether the bank adopted the standardised approach or IRB approach for the measurement of the bank's exposure to credit risk.

J. 1 OPERATIONAL RISK

(All amounts to be rounded off to the nearest '000)

Summary information relating to required capital and reserve funds and risk weighted exposure	Line no.	Gross income			Loans and advances[1]			Relevant risk exposure	Percentage requirement	Capital requirement
		Financial year -3	Financial year -2	Financial year -1	Year -3	Year -2	Year -1			
		1	2	3	4	5	6	7	8	9
Basic indicator approach	292								15%	
Standardised approach[1]: gross income derived from- (total of items 294 to 301)	293									
Corporate finance	294								18%	
Trading and sales	295								18%	
Retail brokerage	296								12%	
Commercial banking	297								15%	
Retail banking	298								12%	
Payment and settlement	299								18%	
Agency services	300								15%	
Asset management	301								12%	
Alternative standardised approach[1] (total of items 303 to 306)	302									
Commercial banking[1, 2]	303								15%	
Retail banking[1, 2]	304								12%	
Commercial banking and retail banking[1, 3]	305								15%	
Business lines other than commercial banking and retail banking[1, 4]	306								18%	
Advanced measurement approach	307									
Capital requirement in respect of operational risk (total of items 292, 293, 302 and 307)	308									
Risk weighted exposure equivalent amount	309									

1. **A bank that obtained the approval of the Authority to apply the alternative standardised approach shall complete items 303 to 306, instead of items 294 to 301. Refer to the relevant directives specified in regulation 33(8)(c).**
2. **Refer to regulation 33(8)(c)(ii)(A).**
3. **Refer to regulation 33(8)(c)(ii)(B).**
4. **Refer to regulation 33(8)(c)(ii)(C).**

J. 2 OPERATIONAL RISK

(All amounts to be rounded off to the nearest '000)

Reconciliation of gross income	Line no.	Financial year -3	Financial year -2	Financial year -1
		1	2	3
Gross operating income (item 137)	310			
Adjustments[1, 2] (total of items 312 to 318)	311			
Income derived from insurance	312			
Operating expenses, including fees paid by the reporting bank to service providers in respect of outsourcing	313			
Realised profits/losses on sale of securities held in the banking book	314			
Impairment	315			
Extraordinary or irregular items	316			
Adjusted prior period errors	317			
Other adjustments (please specify)	318			
Gross income (item 310 minus item 311)	319			
Hash total	320			

1. To the extent that these items are included in item 307 above.

2. Report any relevant expense or other amount to be deducted from gross operating income as a negative amount.

GENERAL NOTICES • ALGEMENE KENNISGEWINGS

SOUTH AFRICAN RESERVE BANK

NOTICE 743 OF 2020

THE BANKS ACT, 1990 (ACT NO. 94 OF 1990 – THE BANKS ACT)

CONSENT GRANTED IN TERMS OF SECTION 54(1)(b) OF THE BANKS ACT

CANCELLATION OF REGISTRATION AS A BANK

Notice is hereby given, for general information, in accordance with the provisions of section 30(1)(f), read with section 30(1)(b)(i) of the Banks Act, that the Minister of Finance, has granted consent for the transfer of all the assets and liabilities of Mercantile Bank Limited to Capitec Bank Limited in terms of section 54(1)(b) of the Banks Act. The registration of Mercantile Bank Limited as a bank was therefore cancelled with effect from 1 December 2020 in accordance with the provisions of section 54(6)(b) of the Banks Act.

DEPARTMENT OF TRADE, INDUSTRY AND COMPETITION

NOTICE 744 OF 2020

STANDARDS ACT, 2008
STANDARDS MATTERS

In terms of the Standards Act, 2008 (Act No. 8 of 2008), the Board of the South African Bureau of Standards has acted in regard to standards in the manner set out in the Schedules to this notice.

SECTION A: DRAFTS FOR COMMENTS

The following draft standards are hereby issued for public comments in compliance with the norm for the development of the South Africa National standards in terms of section 23(2)(a) (ii) of the Standards Act.

Draft Standard No. and Edition	Title, scope and purport	Closing Date
SANS 62930 Ed 1	*Electric cables for photovoltaic systems with a voltage rating of 1,5 kV DC*. Applies to single-core cross-linked insulated power cables with cross-linked sheath.	2021-02-21
SANS 1833-7 Ed 2	*Textiles – Quantitative chemical analysis – Part 7: Mixtures of polyamide and certain other fibres (method using formic acid).* Specifies a method, using formic acid, to determine the percentage of polyamide fibre, after removal of non-fibrous matter, in textiles made of binary mixtures of polyamide with cotton, viscose, cupro, modal, polyester, polypropylene, chlorofibre, acrylic glass fibre elastomultiester, elastolefin and melamine, or wool if the wool content is less than or equal to 25 % or animal hair fibres.	2021-01-03
SANS 105-B01 Ed 2	*Textiles – Tests for colour fastness – Part B01: Colour fastness to light: Daylight.* Specifies a method intended for determining the resistance of the colour of textiles of all kinds and in all forms to the action of daylight.	2021-01-03
SANS 51499 Ed 1	*Chemical disinfectants and antiseptics – Hygienic handwash – Test method and requirements (phase 2/step 2).* Specifies a test method simulating practical conditions for establishing whether a product for hygienic handwash reduces the release of transient microbial flora on hands when used to wash the artificially contaminated hands of volunteers.	2021-02-05
SANS 51500 Ed 1	*Chemical disinfectants and antiseptics – Hygienic handrub - Test method and requirements (phase 2/step 2).* Specifies a test method simulating practical conditions for establishing whether a product for hygienic handrub reduces the release of transient microbial flora on hands when rubbed onto the artificially contaminated hands of volunteers.	2021-02-05
SANS 52791 Ed 1	*Chemical disinfectants and antiseptics – Surgical hand disinfection - Test method and requirements (phase 2, step 2).* Specifies a test method simulating practical conditions for establishing whether a product for surgical handrub and handwash reduces the release of resident and eventually present transient microbial flora on hands when used for the treatment of clean hands of volunteers.	2021-02-05
SANS 52671 Ed 2	*Chemicals used for treatment of water intended for human consumption – Chlorine dioxide generated in situ.*.Describes the characteristics for chlorine dioxide generated on site for treatment of water intended for human consumption.	2021-02-05

SCHEDULE A.1: AMENDMENT OF EXISTING STANDARDS

The following draft amendments are hereby issued for public comments in compliance with the norm for the development of the South African National Standards in terms of section 23(2)(a) (ii) of the Standards Act.

Draft Standard No. and Edition	Title	Scope of amendment	Closing Date
SANS 1507-6 Ed 2.1	*Electric cables with extruded solid dielectric insulation for fixed installations (300/500 V to 1 900/3 300 V) Part 6: Service cables*	Amended to update the sub-clause on UV weathering tests.	2021-02-21
SANS 10198-3 Ed 2.1	*The selection, handling and installation of electric power cables of rating not exceeding 33 kV Part 3: Earthing systems – General provisions*	Amended to delete reference to a national organization.	2021-02-21
SANS 11108 Ed 3.1	*Washing pretreatment of textile fabrics*	Amended to delete references to organizations.	2021-01-03
SANS 1319 Ed 3.2	*Zinc phosphate primer for steel*	Amended to update referenced standards, and to delete the annex on notes to purchasers.	2021-01-03
SANS 11166 Ed 3.1	*Textiles – Colour fastness to domestic washing procedures.*	Amended to delete reference to organizations.	2021-01-03
SANS 10076-2 Ed 2.2	*The assessment of defects in textile piece-goods and made-up articles – Part 2: Defects in woven terry towelling.*	Amended to delete the note on the sub-clause on permissible number of defects, the sub-clause on general, and the notes to purchasers.	2021-02-03
SANS 10076-4 Ed 2.2	*The assessment of defects in textile piece-goods and made-up articles – Part 4: Defects in knitted piece-goods*	Amended to delete reference to organizations and notes to purchasers.	2021-02-03
SANS 10076-6 Ed 2.2	*The assessment of defects in textile piece-goods and made-up articles – Part 6: Defects in woven filament piece-goods*	Amended to delete the note on the sub-clause on permissible number of defects, the footnote on the clause on colour matching, and the notes to purchasers.	2021-02-03
SANS 390 Ed 3.7	*Forks and rakes*	Amended to delete the appendix on notes to purchasers.	2021-02-05
SANS 788 Ed 1.4	*Frozen shrimps (prawns), langoustines and crabs*	Amended to update the clause on microbiological requirements, and to delete the annex on notes to pruchasers.	2021-02-05
SANS 1172 Ed 1.5	*Files and rasps*	Amended to delete the appendix on notes to purchasers.	2021-02-05
SANS 1357 Ed 1.2	*Granite surface plates and tables*	Amended to delete the appendix on notes to purchasers.	2021-02-05
SANS 1110 Ed 1.9	*Screwdrivers for slotted-head screws*	Amended to delete the appendix on notes to purchasers.	2021-02-05

SCHEDULE A.2: WITHDRAWAL OF THE SOUTH AFRICAN NATIONAL STANDARDS

In terms of section 24(1)(C) of the Standards Act, the following published standards are issued for comments with regard to the intention by the South African Bureau of Standards to withdrawn them.

Draft Standard No. and Edition	Title	Reason for withdrawal	Closing Date

SCHEDULE A.3: WITHDRAWAL OF INFORMATIVE AND NORMATIVE DOCUMENTS

In terms of section 24(5) of the Standards Act, the following documents are being considered for withdrawal.

Draft Standard No. and Edition	Title	Reason for withdrawal	Closing Date

SECTION B: ISSUING OF THE SOUTH AFRICAN NATIONAL STANDARDS

SCHEDULE B.1: NEW STANDARDS

The following standards have been issued in terms of section 24(1)(a) of the Standards Act.

Standard No. and year	Title, scope and purport
SANS 11137-2:2020 Ed 2	*Sterilization of health care products – Radiation Part 2: Establishing the sterilization dose.* Specifies methods for determining the minimum dose needed to achieve a specified requirement for sterility and methods to substantiate the use of 25 kGy or 15 kGy as the sterilization dose to achieve a sterility assurance level, SAL, of 10-6.
SANS 15426-2:2020 Ed 2	*Information technology – Automatic identification and data capture techniques – Bar code verifier conformance specification – Part 2: Two-dimensional symbols.* Defines test methods and minimum accuracy criteria applicable to verifiers using the methodologies of ISO/IEC 15415 (published in South Africa under the designation SANS 15415) for multi-row bar code symbols and two-dimensional matrix symbologies, and specifies reference calibration standards against which these should be tested.
SANS 50116:2020 Ed 2	*Diesel and domestic heating fuels – Determination of cold filter plugging point – Stepwise cooling bath method.* Specifies a method for the determination of the cold filter plugging point (CFPP) of diesel and domestic heating fuels using automated test equipment.
SANS 52662:2020 Ed 2	*Liquid petroleum products – Determination of contamination in middle distillates, diesel fuels and fatty acid methyl esters.* Specifies a method for the determination of the content of undissolved substances, referred to as total contamination, in middle distillates, in diesel fuels containing up to 30 % (V/V) fatty acid methyl esters (FAME), and in neat FAME.
SANS 54105:2020 Ed 2	*Fat and oil derivatives – Fatty Acid Methyl Esters (FAME) – Determination of free and total glycerol and mono-, di-, triglyceride content.* Specifies a method to determine the free glycerol and residual mono-, di- and triglyceride contents in fatty acid methyl esters (FAME) intended for addition to mineral oils.
SANS 54112:2020 Ed 2	*Fat and oil derivatives – Fatty Acid Methyl Esters (FAME) – Determination of oxidation stability (accelerated oxidation test).* Specifies a method for the determination of the oxidation stability of fatty acid methyl esters (FAME) at 110 °C, by means of measuring the induction period up to 48 h.
SANS 60947-3:2020 Ed 4	*Low-voltage switchgear and controlgear – Part 3: Switches, disconnectors, switch-disconnectors and fuse-combination units.* Applies to switches, disconnectors, switch-disconnectors and fuse-combination units and their dedicated accessories to be used in distribution circuits and motor circuits of which the rated voltage does not exceed 1 000 V AC or 1 500 V DC.
SANS 61511-3:2020 Ed 2	*Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels.* Provides information on the underlying concepts of risk, the relationship of risk to safety integrity, the determination of tolerable risk, and a number of different methods that enable the safety integrity levels for the safety instrumented functions to be determined.

SCHEDULE B.2: AMENDED STANDARDS

The following standards have been amended in terms of section 24(1)(a) of the Standards Act.

Standard No. and year	Title, scope and purport
SANS 815-2:2020 Ed 1.2	*Shoulder-ended and groove-ended pipe systems – Part 2: Groove-ended steel pipes, fittings and couplings. Consolidated edition incorporating amendment No.2.* Amended to update referenced standards, the requirements for forged steel couplings, and to delete the annex on notes to purchasers.
SANS 1327:2020 Ed 1.5	*Electrical connectors for towing and towed vehicles (7-pole connectors). Consolidated edition incorporating amendment No.5.* Amended to update referenced standards, and the figures on socket type 24N7 and on plug type 24N7.
SANS 10257:2020 Ed 1.3	*The reconditioning of valves for use with pipelines. Consolidated edition incorporating amendment No.3.* Amended to move the reference to legislation to the foreword, to delete the annex on notes to customers, and to update referenced standards.

SCHEDULE B.3: WITHDRAWN STANDARDS

In terms of section 24(1)(C) of the Standards Act, the following standards have been withdrawn.

Standard No. and year	Title

If your organization is interested in participating in these committees, please send an e-mail to Dsscomments@sabs.co.za for more information.

SCHEDULE 5: ADDRESS OF THE SOUTH AFRICAN BUREAU OF STANDARDS HEAD OFFICE

Copies of the standards mentioned in this notice can be obtained from the Head Office of the South African Bureau of Standards at 1 Dr Lategan Road, Groenkloof, Private Bag X191, Pretoria 0001.

DEPARTMENT OF TRANSPORT

NOTICE 745 OF 2020

AIR TRAFFIC AND NAVIGATION SERVICES COMPANY SOC LIMITED

AIR TRAFFIC AND NAVIGATION SERVICES COMPANY ACT, 1993 (ACT No. 45 OF 1993)

PUBLICATION OF AIR TRAFFIC SERVICE CHARGES

In terms of section 5(2)(f) of the Air Traffic and Navigation Services Company Act, 1993 (Act No. 45 of 1993), it is hereby published for general notice that as from **1 April 2021** the Air Traffic and Navigation Services Company SOC Limited, registration number 1993/004150/06, will levy the air traffic service charges according to the rules set out in the Schedule.

S THOBELA

Chairman: Board of Directors

December 2020

SCHEDULE

AIR TRAFFIC SERVICE CHARGES

1. Interpretation

For the purposes of these Rules, unless the context indicates otherwise –

(a) "ACSA" means Airports Company South Africa SOC Limited;

(b) "ACSA airport" means a company airport as defined in section 1 of the Airports Company Act;

(c) "ACSA TMA airspace" means TMA airspace associated with an ACSA airport, but in which may also be non-ACSA airports;

(d) "AIC" means an Aeronautical Information Circular;

(e) "AIP" means an Aeronautical Information Publication;

(f) "Aircraft" means any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the surface of the earth, and includes any non-type certificated aircraft;

(g) "Airport" means an aerodrome as defined in section 1 of the Civil Aviation Act, 2009 (Act No. 13 of 2009), and includes an ACSA airport;

(h) "Airports Company Act" means the Airports Company Act, 1993 (Act No. 44 of 1993), as amended;

(i) "Air traffic control unit" means an aerodrome control tower, an approach control office or an area control centre or a combination thereof;

(j) "Air Traffic Management (ATM) services" includes without limitation –

(i) airspace organization and management services;
(ii) information management services;
(iii) alerting services;

(iv) advisory services;
(v) conflict management services;
(vi) traffic synchronization services;
(vii) flight information services; and
(viii) demand and capacity balancing services;

(k) "Air traffic service charge" means an amount levied by the Company on the operator of an aircraft in connection with the provision of air traffic services to that operator;

(l) "Air traffic service reporting office" means an air traffic service unit established for the purpose of receiving reports concerning air traffic services and flight plans submitted before the departure of an aircraft from an aerodrome;

(m) "Air traffic service unit" means an air traffic control unit, flight information centre or air traffic service reporting office;

(n) "Alerting service" means a service provided to notify the appropriate organizations regarding aircraft in need of search and rescue aid and to assist such organizations as appropriate;

(o) "Area (*en route*) airspace" means airspace that excludes –

(i) aerodrome airspace;
(ii) TMA airspace; and
(iii) FIS-only airspace, when the Company has determined its dimensions;

(p) "ATM" means Air Traffic Management;

(q) "BSC" means business sustaining cost;

(r) "Civil Aviation Regulations" means the Civil Aviation Regulations, 1997, as amended;

(s) "Company" means Air Traffic and Navigation Services Company SOC Limited;

(t) "Company representative" means a person designated by the Company for the purposes of these Rules;

(u) "d" means flight distance;

(v) "FAOR" means OR Tambo International Airport;

(w) "FAKN" means Kruger Mpumalanga International Airport;

(x) "FARB" means Richards Bay Airport;

(y) "FC" means fixed cost;

(z) "FIS-only airspace" means airspace in which flight information services are provided exclusively;

(aa) "Flight" means from the moment an aircraft commences its take-off until the moment it completes its next landing;

(bb) "Flight information centre" means an air traffic service unit established to provide flight information services and alerting services;

(cc) "Flight information service" means a service provided for the purpose of giving advice and information useful for the safe and efficient conduct of flights;

(dd) "Flight plan" means specified information provided to air traffic service units relative to an intended movement of an aircraft;

(ee) "Gateway" means the point of entry into or exit from the South African flight information region;

(ff) "Maximum Certificated Mass" means the maximum permissible mass shown in the aircraft flight manual or other document associated with the certificate of airworthiness at which an aircraft may commence its take-off under standard atmospheric conditions at sea level;

(gg) "MCM" means Maximum Certificated Mass;

(hh) "Movement" means a flight, or a portion of a flight, through any aerodrome airspace, TMA airspace or area (*en route*) airspace;

(ii) "Non-type certificated aircraft" means any aircraft that does not qualify for the issue of a certificate of airworthiness in terms of Part 21 of the Civil Aviation Regulations and includes any type certificated aircraft that has been scrapped, of which the original identification plate has been removed and returned to the applicable aviation authority and is rebuild as a full-scale replica;

(jj) "NOTAM" means a Notice to Airmen;

(kk) "Operator" means a person or legal entity, holding a valid license and operating certificate or equivalent thereof authorizing such person or entity to conduct scheduled, non-scheduled or general air services, and includes –

(i) a licensee as defined in section 1 of the Air Services Licensing Act, 1990 (Act No. 115 of 1990), as amended, or a licensee as defined in section 1 of the International Air Services Act, 1993 (Act No. 60 of 1993), as amended;
(ii) any airline of another State which operates a scheduled international public air transport service in terms of an air transport service agreement as contemplated in section 35(1) of the International Air Services Act, 1993, as amended, or a permit holder as defined in section 1 of the said Act;
(iii) the registered owner of such aircraft; and
(iv) any person or legal entity who uses an aircraft on behalf of an operator;

(ll) "Registered owner", in relation to an aircraft, means the person in whose name such aircraft is registered, and includes any person who is or has been acting as agent in South Africa for a foreign owner, or any person by whom the aircraft is hired at the time;

(mm) "Regulating Committee" means the Regulating Committee established by section 11 of the Airports Company Act;

(nn) "South African flight information region" means the geographical area consisting of the flight information regions of Johannesburg, Cape Town and Johannesburg Oceanic;

(oo) "South African Maritime and Aeronautical Search and Rescue Act" means the South African Maritime and Aeronautical Search and Rescue Act, 2002 (Act No. 44 of 2002);

(pp) "Standard Terms and Conditions" are the terms and conditions of payment set out on the invoice;

(qq) "State aircraft" means aircraft used in military, customs and police services;

(rr) "Terminal control area" means a control area normally established at the confluence of air traffic service routes in the vicinity of one or more ACSA airports as published in an AIP, AIC or NOTAM and designated as a terminal control area;

(ss) "TMA" means terminal control area; and

(tt) "VC" means variable cost.

2. Right to levy air traffic service charges

The Company is entitled to levy the air traffic service charges by virtue of a permission issued by the Regulating Committee on 6 August 2018 for the period from 1 April 2019 to 31 March 2023 in terms of section 11(5) of the Air Traffic and Navigation Services Company Act, 1993.

3. Air traffic service charges

3.1 There are three air traffic service charges:

(a) An Aerodrome Charge, payable for ATM services, specific to aerodrome airspace and maneuvering area, provided by the Company in respect of a flight that takes off from or lands at an ACSA airport;

(b) a TMA Access Charge, payable for ATM services, specific to terminal airspace, provided by the Company in respect of a flight that departs from or arrives at ACSA TMA airspace, where the airport of origin or destination is within that ACSA TMA airspace;

(c) an Area Charge, payable for ATM services specific to area (*en route*) airspace provided by the Company in respect of a flight undertaken within a flight information region established by the Commissioner for Civil Aviation in terms of the Civil Aviation Regulations.

4. Cost components

4.1 Charges consist of the following cost components:

(a) A variable cost component (VC);

(b) a business sustaining cost component (BSC); and

(c) a fixed cost component (FC).

4.2 VCs are treated as follows:

(a) VCs are charged for each flight undertaken at a standard rate per movement;

(b) VCs are the same for Aerodrome Charges, TMA Access Charges and Area Charges.

4.3 BSCs are treated as follows:

(a) BSCs are charged for each movement undertaken in relation to the MCM of an aircraft;

(b) BSCs are the same for Aerodrome Charges, TMA Access Charges and Area Charges.

4.4 FCs are treated as follows:

(a) FCs are charged for each movement undertaken in relation to the MCM of an aircraft, and for Area Charges, also in relation to d within Company managed airspace;

(b) Aerodrome Charges, TMA Access Charges and Area Charges each have a unique FC.

5. Independent variables

For purposes of charging, the independent variables of the tariff formulas set out in the Appendix are the following:

(a) Published MCM expressed in kilograms;

(b) "d", measured on the basis of the great circle distance in nautical miles (rounded to the nearest nautical mile) along that portion of the flight path of an aircraft, which is within the boundaries of the South African flight information region, from the take-off airport or gateway to the landing airport or gateway. It excludes distance flown in the ACSA TMA airspace above the take-off or landing airport or the TMA airspace above FAKN or

FARB, which TMA airspace is for charging purposes a radius of 35 nautical miles around the airport, irrespective of the actual radius.

6. Mass categories

6.1 Subject to the exceptions described in rules 6.2 and 6.3 below, the following aircraft mass categories apply:

(a) Aircraft with a MCM of 15 000 kilograms or less are charged as follows:

(i) VC per movement;
(ii) BSC based on MCM; and
(iii) FC based on MCM, and for Area Charge, also based on d, but no Area Charge is levied if d equals zero;

(b) aircraft with a MCM of more than 15 000 kilograms are charged as follows:

(i) VC per movement;
(ii) BSC based on the square root of MCM; and
(iii) FC based on the square root of MCM, and for Area Charge, also based on d, but no Area Charge is levied if d equals zero.

6.2 Charges for aircraft with a MCM of 5 000 kilograms or less are zero-rated with respect to –

(a) Area Charges; and

(b) Aerodrome Charges or TMA Access Charges at ACSA airports or ACSA TMA airspace other than FAOR subject to the operators of such aircraft adhering to operating procedures around non-FAOR airports as the Company may establish from time to time.

6.3 For aircraft with a MCM of 5 000 kilograms or less at FAOR, the FC components that would otherwise have applied, are replaced with –

(a) a minimum FC in the calculation of the Aerodrome Charge; and

(b) a minimum FC in the calculation of the TMA Access Charge.

7. Formulas and coefficients

Subject to these Rules, the tariff formulas and tariff coefficients are set out in the Appendix attached.

8. Payment of air traffic service charges and security deposits

8.1 Any document produced by the Company on which it is recorded that an ATM service was provided is deemed to be sufficient evidence that the ATM service was indeed provided.

8.2 The operator of an aircraft which is engaged in a flight in respect of which the operator is liable to pay an air traffic service charge in terms of these Rules and in the case where the flight –

(a) terminates at an ACSA airport, must pay the air traffic service charge to the Company representative at that ACSA airport before that aircraft is to take off from that ACSA airport;

(b) commences at an ACSA airport and terminates at an airport other than an ACSA airport, must pay the air traffic service charge to the Company representative at that ACSA airport before that aircraft is to take off from that ACSA airport;

(c) commences and terminates at airports other than ACSA airports, must pay the air traffic service charge to the Company within 30 days of receipt of an invoice from the Company in respect of the air traffic service charge,

unless the operator has previously entered into an agreement with the Company for payment.

8.3 The operator of an aircraft shall –

(a) deposit with the Company an amount, or

(b) provide the Company with a letter of guarantee by a financial institution in a format acceptable to the Company that an amount has been set aside,

as security against the risk of default on payment.

8.4 The Company shall determine the amount referred to in section 8.3 with reference to the actual or expected invoices of an operator, which amount shall be limited to the maximum amount of two months' invoicing.

8.5 The Company may annually revise, and an operator may annually apply for a revision of the amount in section 8.3, with reference to actual or expected invoicing.

8.6 No interest is payable by the Company on any deposit or letter of guarantee held by it in terms of these Rules.

8.7 The Company may charge interest on an outstanding invoice as provided for in the Standard Terms and Conditions.

8.8 The Company is not obliged to withdraw, modify or reissue an invoice after six months from the date of the invoice.

9. General rules, exemptions and exceptions

9.1 The tariffs set out in these Rules, including the Appendix, are exclusive of Value-Added Tax and are therefore subject to the appropriate rate applicable to any specific tariff.

9.2 Air traffic service charges are payable by the operator of an aircraft to the Company.

9.3 Air traffic service charges are payable in respect of South African and foreign state aircraft, unless other provision has been made by means of an agreement with the Company.

9.4 Air traffic service charges are payable in respect of helicopters, except at FAOR where no TMA Access Charge is levied.

9.5 No air traffic service charge is payable in respect of an aircraft engaged in any flight for the calibration of any air navigation infrastructure.

9.6 Air traffic service charges are payable in respect of an aircraft engaged in emergency medical service operations, unless exempted on a case-by-case basis by means of an agreement with the Company.

9.7 Subject to rule 9.9 below, no air traffic service charge is payable in respect of an aircraft requisitioned for and engaged in search and rescue operations in terms of the South African Maritime and Aeronautical Search and Rescue Act.

9.8 Air traffic service charges are payable in respect of an aircraft engaged in search and rescue operations, which aircraft has not been requisitioned in terms of the South African Maritime and Aeronautical Search and Rescue Act, unless exempted on a case-by-case basis by means of an agreement with the Company.

9.9 Search mission co-ordination services are payable by the relevant authority or any operator at a rate of **R1,636,82** per hour or part thereof, where these services fall outside of the normal scope of alerting services and assistance to agencies involved in search and rescue operations, in particular where services are activated due to negligence in canceling service requests.

9.10 (a) Aerodrome Charges and TMA Access Charges are payable in respect of Aerodrome and TMA Access movements solely for the purpose of air crew training at a discount of 70% of the applicable standard Aerodrome Charge or standard TMA Access Charge.

(b) Training movements attract charges as follows:

(i) An Aerodrome Charge is levied for each training movement upon take-off and upon landing from or at an ACSA airport, discounted as described in rule 9.10(a) above;

(ii) for a training movement that does not exit the aerodrome airspace, one Aerodrome Charge is levied for each circuit flown, discounted as described in rule 9.10(a) above; and

(iii) for a training movement that exits the aerodrome airspace into TMA airspace, rule 9.10(b)(i) above applies for each take-off and each landing, and a TMA Access Charge is levied for each circuit flown within the TMA airspace.

(c) For the purposes of this rule, the words "take-off" and "landing" are construed to include the use of ATM services required for take-off and landing.

9.11 For oceanic flights over the Indian Ocean or the Atlantic Ocean within the South African flight information region, including those to and from Antarctica, the FC component of the Area Charge is 50% of the standard Area Charge.

9.12 Extended air traffic service charges at a rate of **R3,273,63** per hour or part thereof, are payable by an operator for the extension of existing air traffic services beyond the normal negotiated and planned service amendments as documented in the Integrated Aeronautical Information Package (IAIP).

9.13 No Area Charge is payable in respect of any aircraft engaged in a flight that takes off and lands at the same airport.

9.14 The Company reserves the right to exempt the operator of an aircraft from payment of, or discount, any of the air traffic service charges if the Company is satisfied that the application of these Rules would amount to an unfair repetition of the same charge.

10. Withholding of services

The Company may withhold services –

(a) until such time that the operator provides evidence to the Company that the deposit or guarantee referred to in section 8.3 has been provided, or

(b) if the operator has failed to settle an invoice as per the Standard Terms and Conditions.

APPENDIX
TARIFF FORMULAS AND COEFFICIENTS

1. An air traffic service charge is composed of the sum of VC, BSC and FC for each discrete Aerodrome, TMA Access and Area movement undertaken, according to the following mass categories and locations:

Main Mass Category	Cost Component	Formulas & Coefficients		
		Aerodrome Charge	TMA Access Charge	Area Charge
FAOR ≤ 5 000 kg	VC	R32.28	R32.28	
	BSC	R131.17/10 000.MCM	R131.17/10 000.MCM	
	FC	R69.20	R127.85	
5 000 kg < MCM ≤ 15 000 kg	VC	R32.28	R32.28	R32.28
	BSC	R131.17/10 000.MCM	R131.17/10 000.MCM	R131.17/10 000.MCM
	FC	R138.43/10 000.MCM	R25.57/1 000.MCM	R18.34/100 000.MCM.d
> 15 000 kg	VC	R32.28	R32.28	R32.28
	BSC	R160.62/100. √MCM	R160.62/100. √MCM	R160.62/100. √MCM
	FC	R169.56/100. √MCM	R313.18/100. √MCM	R224.82/10 000. √MCM.d

2. Each Rand-value coefficient in the table above is multiplied by –

(a) 100% for a domestic flight;
(b) 100% for a regional flight: and
(c) 100% for an international flight,

except in the case of FCs for Aerodrome and TMA Access Charges at FAOR for aircraft with MCM ≤ 5 000 kg where the coefficient as stated in the table applies.

3. As an illustration, assume the following flights:

Example 1

Domestic flight from FAOR to FACT, with aircraft with MCM = 100 000 kg and d = 686 miles

Charge = [Aerodrome Charge at FAOR + TMA Access Charge at FAOR + Area Charge + TMA Access Charge at FACT + Aerodrome Charge at FACT] x 100%

= $[[VC_{Aero} + BSC_{Aero} + FC_{Aero}] + [VC_{TMA} + BSC_{TMA} + FC_{TMA}] + [VC_{Area} + BSC_{Area} + FC_{Area}] + [VC_{TMA} + BSC_{TMA} + FC_{TMA}] + [VC_{Aero} + BSC_{Aero} + FC_{Aero}]]$ x 100%

= [[R32.28 + (R160.62/100 x √100 000) + (R169.56/100 x √100 000)] + [R32.28 + (R160.62/100 x √100 000) + (R313.18/100 x √100 000)] + [R32.28 + (R160.62/100 x √100 000) + (R224.82/10 000 x √100 000 x (686-35-35))] + [R32.28 + (R160.62/100 x √100 000) + (R313.18/100 x √100 000)] + [R32.28 + (R160.62/100 x √100 000) + (R169.56/100 x √100 000)]] x 100%

= [(R32.28 x 5) + (R160.62/100 x √100 000 x 5) + (R160.62/100 x √100 000 x 2) + (R313.18/100 x √100 000 x 2) + (R224.82/10 000 x √100 000 x 616)] x 100%

= R10,133.55

Example 2

International flight from FAOR to international gateway, with aircraft with MCM = 4 500 kg and d = 211 miles

Charge = [Aerodrome Charge at FAOR + TMA Access Charge at FAOR] x 100%

= [[VC_{Aero} + BSC_{Aero}] x 100% + FC_{Aero}] + [[VC_{TMA} + BSC_{TMA}] x 100% + FC_{TMA}]

= [[R32.28 + (R131.17/10 000 x 4 500)] x 100% + R69.20] + [[R32.28 + (R131.17/10 000 x 4 500)] x 100% + R127.85]

= [(R32.28 x 2) + (R131.17/10 000 x 4 500 x 2)] x 100% + R69.20+ R127.85

= R379.66

DEPARTMENT OF TRANSPORT

NOTICE 746 OF 2020

INTERNATIONAL AIR SERVICE ACT, (ACT NO.60 OF 1993)
GRANT /AMENDMENT OF INTERNATIONAL AIR SERVICE LICENSE

Pursuant to the provisions of section 17 (12) of Act No.60 of 1993 and Regulation 15 (1) and 15 (2) of the International Air Regulations,1994, it is hereby notified for general information that the applications, detail of which appear in the Schedules hereto, will be considered by the International Air Services Council (Council) Representation in accordance with section 16(3) of the Act No. 60 of 1993 and regulation 25(1) of International Air Services Regulation, 1994, against or in favour of an application, should reach the Chairman of the International Air Services Council at Department of Transport, Private Bag X 193, Pretoria, 0001, within 28 days of the application hereof. It must be stated whether the party or parties making such representation is / are prepared to be represent or represented at the possible hearing of the application.

APPENDIX I

(A) Full name, surname and trade name of the applicant. (B) Full business or residential address of the applicant. (C) Class of licence applied for. (D) Type of International Air Service to which application pertains. (E) Category or kind of aircraft to which application pertains. (F) Airport from and the airport to which flights will be undertaken. (G) Area to be served. (H) Frequency of flight.

(A) Cape Town Airlines (Pty) Ltd; Escape Airways. (B) Unit 12 Provden Park 2, Aviation Crescent, Airport City, Western Cape, 7525. (C) Class II. (D) Type N1 & N4. (E) Category A1. (F) Cape Town International Airport & O. R. Tambo International Airport.

(A) Van Den Berg Lugbespuiting CC. (B) 28 D'Arcy Street, Douglas, Nothern Cape. (C) Class III. (D) Type G5 & G8. (E) Category A3 & A4. (F) Northern Cape.

(A) Vharanani Aviation (Pty) Ltd; Vharanani Aviation. (B) 18 Hume Road, Dunkeld West, Johannesburg, 2196. (C) Class II. (D) Type N1 & N4. (E) Category A1 & A2. (F) (G) OR Tambo International Airport, King Shaka International Airport, Cape Town International Airport, Lanseria International Airport & Polokwane Airport.

APPENDIX II

(A) Full Name and trade name of the applicant. (B) Full business or residential address of the applicant. (C) The Class and number of license in respect of which the amendment is sought (D) Type of air service and the amendment thereto which is being applied for (E) Category of aircraft and the amendment thereto which is being applied for.

(A) Absolute Flight Services (Pty) Ltd. (B) Hangar103, South Side, Lanseria International Airport. (C) Class II; N964D. (D) Type N1 & N2. (E) Category A1, A2 & A3. **Changes to the MP:** R Grove` replaces R. Geldenhuys as the RP: Aircraft.

(A) Airwork Africa (Pty) Ltd. (B) Suite 4, Hangar 38, Wonderboom Airport, Pretoria, (C) Class II & III; N1162D & G1163D. (D) Type N1, N2, G3, G7, G8, G15 & G16 (Ship to Shore). (E) Category H1 & H2. Changes to the MP: Anine Bothman is appointed as the Air Service Safety Officer & Quality Assurance Manager & Tavia van Deventer as the RP: Flight Operations.

(A) Comair Flight Services (Pty) Ltd: Comair Flight Services / CFS. (B) Hangar 106, Gate 14 (South Side), Lanseria International Airport. (C) Class II; N1015D. (D) Type N1 & N2. (E) Category A1, A2, A3 & A4. **Changes to the MP:** R. B. Ives replaces A. Steyn as the RP: Flight Operations & P. R. Groves replaces A. Reeves as the RP: Aircraft

(A) Fireblade Aviation (Pty) Ltd; Fireblade Aviation. (B) L6 Denel Precinct, Astro Park Atlas Road, Bonaero Park.(C) Class II; I/N274. (D) Type N1 & N4. (E) Category A1, A2, A3, H1 & H2. (F). O. R. Tambo International Airport. **Change in the Controlling Shareholding:** Fireblade Aviation Holdings has 74% & E. M. Dipico Family Trust has 26%.

DEPARTMENT OF TRANSPORT

NOTICE 747 OF 2020

AIR SERVICE LICENSING ACT, 1990 (ACT NO.115 OF 1990) APPLICATION FOR THE GRANT OR AMENDMENT OF DOMESTIC AIR SERVICE LICENCE

Pursuant to the provisions of section 15 (1) (b) of Act No. 115 of 1990 and Regulation 8 of the Domestic Air Regulations,1991, it is hereby notified for general information that the application detail of which appear in the appendix, will be considered by the Air Service Licensing Council. Representation in accordance with section 15 (3) of the Act No.115 of 1990 in support of, or in position, an application, should reach the Air Service Licensing Council. Private Box X 193, Pretoria, 0001, within 21 days of date of the publication thereof.

APPENDIX I

(A) Full name and trade name of the applicant. (B) Full business or residential address of the applicant. (C) Class of licence applied for. (D) Type of air service to which application applies. (E) Category of aircraft to which application applies.

(A) Fusilium 51 (Pty) Ltd. (B) 18 Central Ave, Kempton Park, 1619. (C) Class III. (D) Type G3, G4 & G16 (RPAS). (E) Category H1.

(A) KwaZulu Natal Nature Conservation Board; Ezemvelo KZN Wildlife. (C) Class III. (D) Type G3, G4 & G16 (RPSA). (E) Categoryt H1.

APPENDIX II

(A) Full Name and trade name of the applicant. (B) Full business or residential address of the applicant. (C) The Class and number of license in respect of which the amendment is sought (D) Type of air service and the amendment thereto which is being applied for (E) Category of aircraft and the amendment thereto which is being applied for.

(A) Agiso Aerial Services (Pty) Ltd. (B) 6 East Street, Halfway Gardens, Midrand, 1686. (C) Class III; G1422D. (D) Type G3, G4 & G16 (RPAS). (E) Category A4, H1 & H2. **Changes to the MP:** Matheri Kangethe is appointed as theCEO, Daniel Mwape as the RP: Flight Operations, Mercy Matheri as the Air Service Safety Officer & Jennifer Weru as the Quality Assurance Manager

(A) Rocketmine (Pty) Ltd; Rocketmine. (B) Willow Wood Office Park, Block B, Unit 4, Cnr 3rd & Cedar Avenue. Fourways, Johannesburg. (C) Class III; G1279D. (D) Type G3, G4, G8, G10 & G16 (RPAS). (E) Category A4, H1 & H2. **Changes to the MP:** C. Clark is appointed as the Accountable Manager, A. Harduth as the RP: Flight Operations RP: Aircraft & N. Kgoe as the Air Service Safety Officer

(A) Fireblade Aviation (Pty) Ltd; Fireblade Aviation. (B) L6 Denel Precinct, Astro Park Atlas Road, Bonaero Park. (C) Class II; N1153D. (D) Type N1 & N2. (E) Category A1, A2, A3, H1 & H2. **Change in the Controlling Shareholding:** Fireblade Aviation Holdings has 74% & E. M. Dipico Family Trust has 26%.

(A) Parthenius Air (Pty) Ltd. (B) Bekker RoadXtraSpace Building, Midrand, 1686. (C) Class III; G1424D. (D) Type G3, G4, G10 & G16 (RPAS). (E) Category H1. **Changes to the** MP: Itumeleng Mokoena replaces Thobekile Luthuli as the RP: Flight Operations & Tandile Mthandi replaces Itumeleng Mokoena as the Security Manager, **change of the Company name:** Parthenius Project Consultants (Pty) Ltd to Parthenius Air (Pty) Ltd & **addition of category** A4.

SACPCMP

The South African Council for the Project and Construction Management Professions

CONSTRUCTING NEW PERSPECTIVES

AMENDMENT TO BOARD NOTICE 200 OF 2019

Amendment to Board Notice published in the Government Gazette Board Notice No 200 of 06 December 2019 with regards to the Fees and charges for the calendar year 1 January 2020 to 31 December 2020 in terms of the Project and Construction Management Professions (Act 48 of 2000)

Fees and charges for the financial year 01 April 2020 to 31 March 2021 in terms of the Project and Construction Management Professions (Act 48 of 2000)

The South African Council for the Project and Construction Management Professions (SACPCMP) is empowered in terms of Section 12 (1) of the Project and Construction Management (Act 48 of 2000) to determine fees and charges payable to the Council. The relevant prescribed fees are set out in the schedule below and come into effect on 1 January 2020 to 31 March 2021.

SCHEDULE: Interpretation

The South African Council for the Project and Construction Management Professions hereby prescribes its schedules of fees for the period 1 January 2020 to 31 March 2021.

1. Persons registered with the Council in terms of the Act, are required to pay the applicable Annual fee in January annually.
2. In terms of section 20(1) (a) (iii) of the Act the council may cancel the registration of a registered persons if he/she fails to pay the prescribed annual fee or portion thereof within 60 days of it becoming due or within such further period as the Council may allow, either before or after the expiry of the 60 days
3. A registered person, whose registration has been cancelled in terms of clause 2 above, is liable to pay all arrear annual fees and outstanding fees and all applicable charges on application of reinstatement
4. An Administrative fee will be charged should the applicable annual fee not be paid within the prescribed period
5. The annual fee for initial registration is calculated on a pro-rata dependent on which month of the year registration takes place.

The fees prescribed herein include Value Added Tax (VAT)

CATEGORY	APPLICATION FEE	INTERVIEW FEE	EXAMINATION FEE	REGISTRATION FEE	ANNUAL FEES
Professional (Pr. CM. Pr. CPM, Pr. CMe)	R2 511.52	R4 142.90		R1 281.56	R4 168.77
Candidate (C. CM, C. CPM)	R2 511.52			R1 281.56	R3 226.30
Specified Category: Construction Mentor	R2 511.52	R4 142.90		R1 281.56	R3 758.71
Professional Construction Health and Safety Agent	R2 511.52	R4 142.90		R1 281.56	R4 168.77

Construction Health and Safety Manager	R992.92		R1 159.59	R1 254.51	R3 515.56
Construction Health and Safety Officer	R314.79		R551.32	R275.65	R2 947.83
Candidate Construction Health and Safety	R273.73			R270.52	R2 635.91

OTHER APPLICABLE FEES	
Voluntary Association – Annual Fee	R4 951.05
Administrative Fee - Professionals	10% of outstanding
Administrative Fee - Candidates	10% of outstanding
Privy Seal fee	R17.25
RPL – (Pr. CM, Pr. CPM, Pr. CMe)	R15 040.00
RPL – (CHSM, CHSO)	R9 661.03
Assessment of logbooks (C. CM, C. CPM)	R573.92
Assessment of Logbooks Candidate CHS	R241.81
Appeals Fee	R6 000
CBE Levy (Professional)	R48.30
CBE Levy (Candidate)	R24.15

CPD BUNDLES	
CPD BUNDLE 1	R1 512.25
CPD BUNDLE 2	R1 512.25
CPD BUNDLE 3	R1 512.25
CPD BUNDLE 4	R1 512.25
CPD BUNDLE 1-4	R4 234.30
CPD BUNDLE 1-3	R3 175.73
CPD BUNDLE 1-2	R2 117.15

PROGRAMME ACCREDITATION CATEGORY	
Description	**Fees**
Re-accreditation of Existing Programmes	R86 087.68
Paper-based Assessment	R25 804.78
CHS Skills Modules	R5 021.78

BANKING DETAILS

BANK : NEDBANK
ACC NAME : The SA Council for the Project and Construction Management Professions
ACC NO : 128 406 4557
BRANCH : BUSINESS CENTRAL
BRANCH CODE : 128 405
The document is downloadable from: www.sacpcmp.org.za