Joint Standard: IT Governance and Risk Management requirements

Consultation Report

November 2022

1. Purpose

1.1 Section 104 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) (FSR Act) states that with each regulatory instrument, the maker must publish a consultation report which must include:
(a) a general account of the issues raised in the submissions made during the consultation; and
(b) a response to the issues raised in the submissions.

1.2 The purpose of this document is to set out, as required in terms of section 104 of the FSR Act, a report on the consultation process undertaken in respect of the **Joint Standard: IT Governance and Risk Management requirements.**

2. Summary of consultation process and general account of issues raised

2.1 On 9 June 2021, the Financial Sector Conduct Authority and Prudential Authority (hereafter jointly referred to as "the Authorities") published the following documents for public comment, with comments due on 26 July 2021:
(a) Notice regarding the publication of draft Joint Standard – IT Governance and Risk Management (Joint Standard) inviting comments on the Joint Standard;
(b) The draft Joint Standard;
(c) Statement of the need for, intended operation and expected impact of the proposed Joint Standard on information technology governance and risk management; and
(d) A comment template.

2.2 The Authorities received over 600 comments from 32 respondents. Following the public consultation process, where appropriate, certain comments resulted in amendments being made to the Joint Standard by the Authorities. The amendments were not deemed to be material.

2.3 A general account of issues raised during the consultation process and the response of the Authorities are tabulated in Table 1 below. Details of commentators and the full set of comments and responses are detailed below in Table 2 and Table 3 below.

2.5 Based on the number of comments received during the consultation period, the Authorities conducted, in terms of section 101 of the FSR Act, targeted consultation with the commentators from the original consultation period to solicit comments on the amendments made to the Joint Standard. The targeted consultation was conducted in July 2022 with the consultation period ending on 10 August 2022. A general account of the comments received during the targeted consultation and a full matrix of all the comments received are tabulated in Table 4 and Table 5, respectively.

Table 1

Area	Summary of comment	Response from the Authorities
Commencement of the Joint Standard	The commencement date of the Joint Standard, initially proposed as 1 January 2022, was seen as too ambitious for industry and requests were made for more time and an period after finalisation of the Joint Standard for financial institutions to prepare for implementation. Smaller entities may also struggle to meet the compliance deadlines for the Joint Standard.	The Standard comes into effect 12 months after date of publication for financial institutions to prepare for compliance with the Joint Standard
Cost of compliance	The cost of compliance of the Joint Standard may be relatively low to moderate however when aggregated together with the overall cost of compliance and governance, may result in increased pressure on the economic viability of small to medium enterprises. The need for additional staff with the requisite skills has also been identified.	The Authorities as per the requirements of the FSR Act are required to publish a draft statement of need for, intended operation and expected impact of the Joint Standard. These requirements in the Joint Standard were considered in light of the impact and considering the cost of compliance. It is advised however, that the risk of inadequate IT Risk Management framework and strategy may have dire consequences on the entire operation of the financial institution especially as the financial sector operates in a highly digitalised environment.
Definitions	Request for clarity on certain terms used in the Joint Standard.	Clarification was provided on terms. Additional terms were also defined such as data and information asset. Definitions were also expanded on or streamlined in terms of the comments received.
Application of the Joint Standard	Request for clarity on how the requirements of the Joint Standard will apply in terms of financial sector laws and prudential/conduct standards and other instruments that deal with similar subject matter. Clarification on how the Joint Standard apply to groups. Concerns around the prescriptive nature of the Joint Standard. Clarity relating to the provision on the nature, scale and complexity of the financial institution in relation to the application of the Joint Standard. Application of the Joint Standard in addition to other financial sector laws and other legislation such as the Protection of Personal Information Act and Cybercrimes Act.	The Joint Standard applies on a consolidated and solo level and must be read together with financial sector laws and instruments issued thereunder. The other financial sector laws provide basic requirements on risk management and reporting whilst this Joint Standard provides detailed requirements specific to the area of IT Risk Management. Due to the risk posed from operating in a largely digital environment, there is an urgent need to codify minimum regulatory requirements. The nature, scale and complexity provision, relates to more complex entities that will need to do more than the minimum to ensure that the risks are adequately identified, assessed and managed. The Joint Standard applies in addition to the requirements of other pieces of primary legislation.
Roles and responsibilities	Request to change the word 'responsible' to 'accountable' in terms of the duty placed on the	The Authorities hold the board ultimately responsible for ensuring compliance with the Joint Standard. The

	governing body (board) and a new paragraph allowing delegation from the board and senior management. The separation of IT Risk Management from the overall risk management framework seems to be suggested in the Joint Standard. Clarification of the oversight function of the board. Clarity on the role of the lines of defence in terms of the roles and responsibilities.	delegation of responsibility is an internal matter and is not prohibited in terms of the Joint Standard. It is not the intention for IT Risk Management to be separated from the broader risk management framework or enterprise risk management framework and this was subsequently clarified in the Joint Standard. The governing body needs to ensure that an effective risk management framework and strategy is implement. After all, these are board approved frameworks. The Authorities are of the view that lines of defence are defined by the respective financial institution to ensure separation of roles and independence. The lines of defence are not defined by this joint Standard, but by other financial sector law as stated in paragraph 4.4. The financial institutions when detailing responsibilities must align such with the applicable lines of defence in terms of their respective governance and risk management frameworks.
IT Strategy	Clarification on whether a separate IT Strategy is required. Suggestions for the strategy to be reviewed after every three years as opposed to the yearly review required by the Joint Standard. Suggestion for action plans to be reviewed annually or six-monthly rather than quarterly as prescribed by the Joint Standard. The significant cost associated with the quarterly review was also tabled. Clarity on the form and manner in which reporting to the Authorities will be required. Request for reporting to be provided to the responsible authority rather than to both Authorities. Concern that the deviation from IT Strategy is not being classified in terms of materiality and no time period is given for the actual reporting.	The Joint Standard does not prohibit the strategy or risk management related to IT to form part of the enterprise risk management system but that it must be easily identifiable. However, the Authorities are of the view that each business unit must have its own strategy and objectives aligned to the overall organisation strategy. The requirement of the Authorities is that the strategy be reviewed regularly but at least on an annual basis as a strategy needs to be adapted as market conditions, internal conditions and other risk change and evolved. A strategy is dynamic in nature and requires regular review. The action plans review feed into the overall review of the strategy therefore the quarterly review is considered appropriate to track the progress in terms of the overall strategy review, which must be conducted at least on an annual basis. Due to the evolving nature and serious impact of IT risks, in order to ensure relevance and appropriateness, the Authorities believe quarterly reviews of the action plans are appropriate. The form and manner will be determined by the Authorities once the Joint Standard is finalised. The Joint Standard was amended to require reporting to the responsible authority in terms of the financial sector law which the financial institution is registered or licenced and not to both Authorities as previously prescribed. Non-compliance with any provision of this Standard, regardless of materiality, is a contravention of legal requirements. The requirement is therefore that any deviation must be reported. In order to address the concern, wording that “within a reasonable time”, has been insert into the provision.
IT Risk Management Framework	Concern that the Joint Standard implies that a separate of stand-alone IT Risk Management framework is required and does not recognise an IT Risk Management framework within an Enterprise Risk Management Framework. Suggestion for the period of review for the risk management framework be extended to 3 years as opposed to the required 1 year as prescribed in the Joint Standard. Clarifications concerning the annual independent review and the practicality around this requirement. Concerns around the practicality of fit and proper requirements for all contractors and vendors which include aspects such as qualifications and experience.	The Joint Standard was amended to clarify that the IT Risk Management framework may form a component of the Enterprise Risk Management (ERM) framework. Annual reviews provide an opportunity for the financial institution to made amendments based on gaps or inefficiencies in the risk management framework as a result of ever-changing IT risks. The requirement is not for an independent review by external auditors. Since risk changes on a daily basis, the requirement for the framework to be reviewed at least annually is not over prescriptive. Furthermore, the Joint Standard was amended to define ‘independent review’. The requirement to be fit and proper applies only to staff, vendors and contractors who are authorised to access the financial institution’s systems, and only insofar as fit and proper requirements are imposed by a sectoral law. Should a staff member, vendor or contractor not be fit and proper, the financial institution should not allow that person access to its systems. In addition, that person would be in contravention of the requirement of the relevant sectoral law, and the institution would have to follow the necessary steps for dealing with non-compliant persons as provided for in that sectoral law.
Oversight of IR Risk Management	Clarification of the oversight of IT Risk Management at the group or solo level.	The Authorities are of the view that if the financial institution is licensed for more than one activity, each entity licensed must comply based on the size nature

		and complexity irrespective of where controls have been defined from. The minimum requirements are the same for the various financial institutions and the financial institution must apply the principles based on the nature, scale and complexity. With regard to bank controlling companies and insurance group, the requirements apply at a consolidated level and a solo level. Each financial institution captured by this Joint Standard must be able to prove compliance with the requirements on institution-specific risk whether it is captured at an institution level or at a group level.
IT Operations	Requested the unpacking of the word 'framework' to include standards, procedures, policies etc. Concern was raised over the need to seek board approval of operations and processes. The reference to "testing" causes confusion because testing could be integrated in stages of development and be dealt with differently depending on the development process. It is proposed that paragraph 9.5 should be rephrased to require appropriate segregation of duties between development and production environments.	The Joint Standard was amended to unpack the concept of framework in terms of the area of IT operations. This was noted by the Authorities and the need to get board approval for operations and processes was removed from the Joint Standard. This was noted by the Authorities and the paragraph was amended to give effect to the comment.
Information security	Various comments were received on the requirements relating to information security and whether it was suitable for the Joint Standard.	The comment was noted by the Authorities and a decision was made to move the requirements relating to information security to the Joint Standard on Cybersecurity and Cyber Resilience which was published in December 2021 for public consultation.
Sensitive and confidential information	Clarity was requested on independent reviews.	A definition for independent review was inserted.
Risks associated with products and services	Concern was raised on the way the requirement was worded as it may be misinterpreted that the bank will also be responsible for the security of the client's devices/infrastructure they use to connect to banks online systems. Suggest rewording to indicate the bank only being responsible/accountable for what is under its control	The comment was noted but the Authorities are cognisant of the limitations regarding customer protection; however, the expectation is that the financial institutions should implement appropriate and **reasonable** measures to protect the customer. The paragraph has been amended to include 'reasonable'.
System recovery and business interruption	Request for name change of the title of the paragraph to align with industry terminology. Clarity regarding the terminology 'geographically separate' in respect to a recovery site. Application of the requirements to cloud-computing.	The title of the paragraph was changed to 'IT Resilience and business continuity'. It is the view of the Authorities that 'geographically separate' is very clear and a sensible requirement. If the DR and the production sites are within the same proximity, and there are riots and/or disaster in that area, then the financial institution might find it difficult to restore its services. The Authorities are of the view that irrespective of whether an institution uses cloud computing or traditional DR site, the principle is the same. Where cloud computing is preferred, different instances should be geographically separate.
Outsourcing	Various comments were received on the requirements impose on outsourcing and its position within the IT Risk Joint Standard.	The Authorities noted the comments and decided that the area of outsourcing would be better captured under a Joint Standard applicable to the financial institution rather than being limited under the scope of the IT Risk Management Joint Standard. As a result thereof the paragraph was deleted.
Assurance	The paragraph relates to responsibilities placed only internal audit and not on control functions.	The Joint Standard was amended to make the role of the control functions clear in terms of assurance.
Reporting	Concerns about having to report to both Authorities. Clarification was requested on the form and manner of reporting. Clarity was requested about regulatory instruments that currently require reporting e.g. Banks Act Directives.	The Joint Standard was amended to allow financial institutions to report to the responsible authority of the financial sector law in terms of which they are registered or licenced. The reporting returns will be published for comment before they are determined by the Authorities. It is envisaged that the reporting requirements under financial sector laws will be repealed, and reporting will occur under this Joint Standard.
General comments	Request to change the name of the Joint Standard to Information and technology governance. Comments on the impact of the Joint Standard Concerns about conflating technology risk, information risk, cyber risk and information security in one Standard	The Authorities noted the comment and have changed the name of the Joint Standard to be IT Governance and Risk Management. Reference was made to the impact assessment conducted by the Authorities. The Authorities acknowledge that these topics have been covered in this Standard, however it is sometimes not possible to separate. In instances where possible, we have separated the topics. Information security will be covered separately in the Cybersecurity and cyber resilience Joint Standard. Outsourcing will be covered under a separate Joint Standard.

Joint Standard: IT Governance and Risk Management requirements

Commentators and full set of comments

Table 2

No.	Name of organisation	Acronym	Contact person
1.	Association for Savings and Investment - South Africa Consolidated submission on behalf of ASISA Members	ASISA	Johann van Tonder Senior Policy Advisor
2.	Assupol Group Assupol	Assupol	Solly Keetse Group Head: Legal & Compliance, Group Legal Services
3.	AVBOB Mutual Assurance Society	AVBOB	Carl van der Riet Chief Executive Officer
4.	African Bank	African Bank	Piet Swanepoel
5.	AC & E Engineering Underwriting Managers (Pty) Ltd	AC & E	Shaun Grobbelaar – IT Manager
6.	BDO Advisory Services Proprietary Limited Kevin	BDO	Moodley, Director Nevellan Moodley, Director
7.	BNP PARIBAS	BNP Paribas	Bsharat Hussain / Chief Information Security Officer (based in Bahrein) Benoit Pivot / Chief Operating Officer (based in RSA)
8.	BrightRock Life Limited	BrightRock	Gys Els, Chief Risk Officer
9.	Clientèle Group: Clientèle Life Assurance Company Limited, Clientèle General Insurance Limited, CBC Rewards (Pty) Ltd	Clientele	Malcolm Mac Donald Group IT Director
10.	ECIC	ECIS	Mpho Mofokeng
11.	Dotsure Limited	Dotsure	Thapelo Metsileng Head of Compliance
12.	FirstRand Limited	FirstRand	Jace Mudali Head: IT Risk and Governance
13.	GENRIC INSURANCE COMPANY	Generic insurance Company	Stuart Forbes Chief Risk and Compliance Officer
14.	General Reinsurance Africa Limited	Genre	Sharon Burton (Contributor: Frank Schmid, Chief Technology Officer, General Reinsurance Corporation, Stamford, CT, U.S.A.)
15.	Hollard	Hollard	Kaajal Maharaj IT Risk and Governance
16.	HBZ Bank Limited	HBZ Bank	Farooq Anwar, Chief Operating Officer
17.	JSE Ltd	JSE	Anne Clayton, Head Public Policy & Regulatory Affairs
18.	Just Retirement Life South Africa	Just SA	Thiren Pillay – Executive: Head of Risk Management
19.	J. Winston Hayden, CISA, CISM, CGEIT, CRISC, CDPSE	J Hayden	
20.	Maitland Group South Africa Limited	Maitland	Deirdre van der Berg
21.	Masthead (Pty) Ltd	Masthead	Anri Dippenaar / Head of Compliance
22.	Maynard Bester	Maynard Bester	(ISACA member)
23.	Ninety One Assurance Limited, Ninety One Investment Platform, Ninety One SA (Pty) Ltd, Ninety One Fund Managers RF SA (Pty Limited, Ninety One Alternative Investments (Pty) Ltd	Ninety One	Jacqueline Smith – Head of Compliance
24.	Outsurance Insurance Company	Outsurance	Maretha Hurter
25.	PSG Konsult	PSG Konsult	Ronald King – Head: Public Policy & Regulatory Affairs
26.	South African Institute of Stockbrokers	SAIS	Erica Bruce CEO and President
27.	The South African Insurance Association NPC	SAIA	Mashudu Pearl Mabogo Legal Specialist
28.	SAHL Investment Holdings (Pty) Ltd (SA Home Loans Group)	SAHL	Ursula Schei (Group Legal and Compliance Manager)
29.	The Federated Employers Mutual Assurance Company (RF) PTY LTD	FEMA	Mr G M McIntosh Chief Information Officer (CIO)
30.	The Banking Association South Africa	BASA	Adri Grobler
31.	Telesure Investment Holdings (Pty) Ltd	Telesure	Eben Steyn Senior Manager Compliance
32.	Ubank Limited	Ubank	Conrad Theron

Table 3

No	Commentator	Paragraph of the Standard	Comment	Responses
1. Commencement				
1	SAIA		No comment.	Noted
2	Maynard Bester (ISACA member)		No comment.	Noted
3	HBZ Bank	1.1	No comment.	Noted
4	FEMA		No comment.	Noted
5	Generic Insurance		No comment.	Noted
6	JSE		No comment.	Noted
7	Ubank		No comment.	Noted
8	J Hayden		No comment.	Noted
9	Maitland		No comment.	Noted
10	SAHL		No comment.	Noted
11	BNP Paribus		No comment.	Noted
12	SAIS		The proposed commencement date is 1 January 2022. The SAIS is of the opinion that should this standard become a requirement, the proposed commencement date does not provide sufficient time for authorised users to develop and implement the measures as required by the standard. The comments provided in this document support the postponement of the commencement date. An 18-month postponement is proposed i.e. a commencement date of 31 June 2023, should industry accept the proposal. Furthermore, the SAIS requests more consultation and clarity regarding applicability in cases where an authorised user is also an FSP, as licenced under FAIS.	The Authorities have provided 12 months for financial institutions to prepare for the implementation date of the Joint Standard once it has been published. The Joint Standard is only applicable to the financial institutions as defined.
13	PSG Konsult		We believe that the proposed commencement date of 1 January 2022 may be ambitious for industry to have fulfilled all proposed requirements in a fully documented and established way. We therefore propose an extended commencement date.	Refer to response as per comment number 12.
14	Assupol Group		Proposed Feedback to Regulator: The timeline for implementing all controls before the proposed date of January 2022, may not be enough given the current socio-economic situation the world is in. Some of the projects required to comply with the standard will require investment and maturing of processes. With that said, we firmly support the implementation of the joint standard as it aligns to industry best practice that the Assupol Group has strived to meet. However, we'd like to propose the implementation date of July 2023 for the aforementioned reasons.	Refer to response as per comment number 12.
15	BDO	1.1	The cost of compliance of this standard may be relatively low to moderate, however when aggregated together with the overall cost of compliance and governance, may result in increased pressure on the economic viability of small to medium entities. Based on the effective date of the standard, the applicable entities have less than six months to ensure compliance. Whilst the bigger entities may largely be compliant with the standard, the small to medium entities may struggle with meeting the deadline based on the following factors: - The cost associated with implementing this standard; and The need for additional staff with adequate skill and experience to identify and remediate any gaps.	Noted, please refer to the Statement of need for, expected impact and intended operation. Also, the Authorities have provided 12 months for financial institutions to prepare for the implementation date of the Joint Standard once it has been published.
16	ASISA		Compliance with new requirements will not be achievable by 1 January 2022. Financial institutions should be allowed a period of 12 months from the date of the publication of the Joint Standard to review their existing strategies, policies, processes, and procedures against the requirements of the Joint Standard, to identify shortcomings and to make the necessary amendments. It is not feasible to achieve compliance in a shorter time, especially in larger financial services groups where IT policies, processes, and procedures are voluminous.	Refer to response as per comment number 12.
17	ECIC		No objection to the proposed commencement date	Noted, however; the Authorities have provided 12 months for financial institutions to prepare for the implementation date of the Joint Standard once it has been published.

No	Commentator	Paragraph of the Standard	Comment	Responses
18	FirstRand		1 Jan 2022 is the commencement date, If the expected compliancy date is also 1 Jan 2022, the timeframe might not be practical. FirstRand recommends a period of 6 to 12 months to implement following final approval and publication of the standard.	Refer to response as per comment number 12.
19	Masthead	1	In our view the commencement date is too soon for smaller independent FSPs to have sufficient time to analyse, understand and then apply these changes to their organisations. These FSPs would in most instances have to look outside of their organisations to source these services on an outsourced or third-party services basis, which requires additional time for due diligence, contracting, scoping and project planning for implementation. In addition, the financial pressure that this places on these FSPs who are already financially strained by the current social and economic environment, as well as new data and information protection legislation such as the POPI Act, would severely pressurise them. In our view the commencement date should be extended by at least 18 months.	Refer to response as per comment number 12.
20	Ninety-one		It is noted that the proposed commencement date of the Standard is 1 January 2022. This will allow financial institutions an implementation period of less than 6 months, depending when the final Standard is released. We submit that the implementation period should be extended to 9 -12 months from the date of the commencement of the final Standard. This will allow Financial Institutions sufficient time to implement any system upgrades where necessary. It must be born in mind that most financial institutions to which this Standard will apply form part of group infrastructures and there are many other regulatory initiatives to be implemented in addition to the implementation of this Standard.	Refer to response as per comment number 12.
21	BASA		BASA suggests that there should be a grace period of six months from 1 January 2022 to address identified shortcomings, implement the requirements and to not disrupt current initiatives. Consideration should be given to aligning the IT Risk Standard to other Directives/ Requirements related to Operational Risk Management for Financial Institutions: e.g., Losses and Scenarios (when considering IT Risk Insurance etc).	Refer to response as per comment number 12.
22	BASA		Define commencement. Will there be a period to become compliant from that date, or will compliance be enforced from that date?	Refer to response as per comment number 12. The Authorities have provided 12 months for financial institutions to prepare for the implementation date of the Joint Standard once it has been published.
23	Hollard	1.1	The commencement of the standards needs to take into account that organisations will require time to mature to the level of standards expected.	Refer to response as per comment number 12. The Authorities have provided 12 months for financial institutions to prepare for the implementation date of the Joint Standard once it has been published.
24	Telesure	1.1	The commencement date is noted as January 2022. Considering the significant reforms proposed additional time will be required to align with the Standard and implement the various frameworks and processes. We therefore propose that a transitional period be granted of no less than 12 months in order for financial institution to align with the standard.	Noted. Refer to response as per comment number 12.
25	GenRe		1 January 2022 seems very ambitious	Refer to response as per comment number 12.
2. Legislative authority				
26	SAIA		No comments.	Noted.
27	SAIS		No comments.	Noted.
28	PSG Konsult		No comments.	Noted
29	Assupol Group		No comments	Noted
30	Maynard Bester (ISACA member)		No comment.	Noted
31	BDO		No comment	Noted
32	HBZ Bank	2.1	No comment	Noted
33	FEMA		No comment	Noted
34	ASISA		No comment	Noted
35	ECIC		No comment	Noted

No	Commentator	Paragraph of the Standard	Comment	Responses
36	GENERIC Insurance Company		No comment	Noted
37	FirstRand		No comment	Noted
38	JSE		No comment	Noted
39	Ubank		No comment	Noted
40	J Hayden		No comment	Noted
41	Maitland		No comment	Noted
42	SAHL		No comment	Noted
43	BNP Paribus		No comment	Noted
44	BASA		No comment	Noted
45	GenRe		No comment	Noted
3. Definitions				
46	PSG Konsult		No comment	Noted
47	Assupol Group		No comment	Noted
48	Maynard Bester (ISACA member)		No comment	Noted
49	BDO		No comment	Noted
50	FEMA		No comment	Noted
51	GenRe		No comment	Noted
52	ASISA	Definition: **'IT'**	Please refer to comment A above. It is proposed that the wording should be aligned with King IV. --- *'IT' means information and technology;*	The Authorities use the terminology used by standard setters or used in best practice regarding the area of information technology to define terms used in this Joint Standard. The difference between information systems and information technology is that information systems incorporate the technology, people and processes involved with information. Information technology is the design and implementation of information, or data, within the information system. The joint standard is based on information technology which is also complemented by data.
53	ASISA	Definition: **'material incident'**	The term is not used anywhere in the Draft Standard and the definition should therefore be deleted.	The term has been included in paragraph 14 of the Joint Standard.
54	BASA	Material Incident (3.1)	BASA suggests renaming this definition to 'Material **IT** Incident' and to add the words 'system failure' to the definition as follows: "*refers to a system failure,* **resulting in the** *disruption of …".*	It is not necessary to classify material 'IT' incident as a non-IT incident may affect IT systems.
55	ASISA	Definition: **"networks"**	The definition appears to define a network rather than networks. Furthermore, the term 'network' features more prominently in the Standard. The reference to *"networks"* should be replaced with a reference to "*network*".	The Authorities have defined "network" as suggested.
56	FirstRand	'governing body' definition	'Governing body' as defined in the FSR Act would refer to the board of directors in a large financial institution. A majority of the obligations in the proposed standard place compliance obligations (such as approval and review of frameworks) on the 'governing body'. However, in reality these compliance obligations are appropriately dispensed with by way of delegations from the governing bodies to sub-committees. Governing bodies may still have overall oversight or accountability, but consideration should be given to allowing for such delegations where reference is made to specific compliance obligations (apart from the governing body's obligation to have oversight and ultimate accountability). In other words where reference is made to 'governing body', this should be limited to obligations for oversight and ultimate accountability and should not apply to day-to-day operational and compliance functions, which can be appropriately dispensed by senior technical teams, under the delegated authority of executive management.	The governing body has the right to delegate functions to senior management etc. The Authorities however, we regard the board as being ultimately responsible for compliance with this Standard and to provide account for areas that fall within the scope of the board's responsibilities whether they have been delegated or not.
57	BASA	"IT asset"	BASA seeks clarity on whether the definition of "IT asset" excludes data (i.e., only applicable to hardware and software as per current definition).	The IT asset definition excludes data as per definition. The standard does not cover data as there is legislation covering data elements.

No	Commentator	Paragraph of the Standard	Comment	Responses
			BASA suggests that consideration should be given to expanding the definition of "IT environment" to explicitly include cloud, given the increasing adoption of cloud services and integration of cloud environments into institutions' IT environments. BASA also notes that there is no clear distinction between IT Environment and IT Infrastructure and recommends that the definitions be combined into. We note that there are no definitions included to provide for “Data”, “Information”, and “Segmentation”, which are necessary for clear interpretation of some of the requirements in the Standard. We suggest that these definitions should be included to ensure clarity in this regard. The Standard is published in accordance with provisions of the Financial Sector Regulation Act 9 of 2017 (“FSRA”), The definition of “Senior Management” is included in the Standard and is deemed to constitute the: (a) chief executive officer or the person who is in charge of a financial institution; or (b) a person, other than a director or a head of a control function (i) who makes or participates in making decisions that - (aa) affect the whole or a substantial part of the business of a financial institution; or (bb) have the capacity to significantly affect the financial standing of a financial institution; or (ii) who oversees the enforcement of policies and the implementation of strategies approved, or adopted by the governing body; and … “Senior Management” is however not defined in the FSRA and therefore BASA recommends that definition be aligned to the definition of “Key Person” as already provided for in the FSRA and that any reference throughout the Standard to ‘senior management’ should be replaced with “Key Person/s”.	The definition implicitly include cloud based on “external”. The definition is sufficient as it has a phrase “external networks” which includes off premises environment, which refers to both cloud and non-cloud environment The authorities have defined data in the standard. However, Segmentation has not been defined as it has not been used. Furthermore, Information cannot be defined as it is used as a conjoined for different purpose. The reason that a specific definition has been created is that the definitions in the FSRA do not fit the purpose of the requirement for this Joint Standard. Senior management does not include the board and control functions and the definition of key person includes the board and control functions.
58	JSE	‘material IT activity or function'	In this definition the undefined term ‘IT operations’ is used. It is unclear whether it is intended that the term has the same meaning of ‘IT infrastructure’. If it is intended that the terms ‘IT operations’ and ‘IT infrastructure’ have a separate and distinct meaning, we recommend that the term ‘IT operations’ is defined.	The outsourcing paragraph has been deleted and thus this term is no longer used in the Joint Standard and has been deleted.
59	FirstRand	Material IT Activity	The definition of material IT activity should be focused on business criticality of the IT process/function in question rather than the propensity for impact to IT operations which would instead be addressed by the definition of material incident Suggested definition: ‘*material IT activity or function' is defined as that IT element which is deemed critical to the ongoing support of a key business function and/or customer service which has the potential to have a significant impact on the financial institution’s business operations or its ability to manage risks effectively* ***should it be disrupted***;	See response to comment 58.
60	JSE	‘IT infrastructure’	See general comment below in respect of the use of the term “enterprise”.	Noted.
61	JSE	‘RTO’	Missing word: **‘RTO’** is the recovery time objective and means the duration of time, from the point of disruption, within which ~~a~~ an IT system should be restored;	Noted.
62	JSE	‘financial institution’	A market infrastructure is licensed and not registered in terms of the Financial Markets Act 2012 (Act No. 19 of 2012).	Noted, the definition has been amended.
63	BASA	‘financial institution’ (3.1)	BASA notes that the Draft Standard correctly recognised the FSR Act as the “*legislative authority” and notes that “In this Standard, ‘the Act’ means the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) and any word or expression to which a meaning has been assigned in the Act bears the meaning so assigned to it, and unless the context indicates otherwise”* To avoid regulatory confusion, we suggest that the definition of a “financial institution” in this Draft Conduct Standard should align to the definition of a “financial institution” in the FSR Act, which states as follows: 'financial institution' means any of the following, other than a representative: (a) A financial product provider; (b) a financial service provider; (c) a market infrastructure; (d) a holding company of a financial conglomerate; or (e) a person licensed or required to be licensed in terms of a financial sector law Considering there are banks with diversified lines of business some of which do not constitute financial services. The instrument should be flexible in application to parts of	The definition for financial institution provided in the FSR Act is too broad for the purposes of this Joint Standard.

No	Commentator	Paragraph of the Standard	Comment	Responses
			a group constituting a financial institution rather than blanket applicability to all lines of business.	
64	FirstRand	financial institution	This Draft Standard correctly recognised the FSR Act as the “legislative authority” and notes that “In this Standard, ‘the Act’ means the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) and any word or expression to which a meaning has been assigned in the Act bears the meaning so assigned to it, and unless the context indicates otherwise” To avoid regulatory confusion, we suggest that the definition of a “financial institution” in this Draft Conduct Standard should align to the definition of a “financial institution” in the FSR Act, which states as follows: *'financial institution' means any of the following, other than a representative:* *(a) A financial product provider.* *(b) a financial service provider.* *(c) a market infrastructure.* *(d) a holding company of a financial conglomerate; or* *(e) a person licensed or required to be licensed in terms of a financial sector law*	Refer to the response per comment 62.
65	BASA	Fit and Proper requirements (3.1)	BASA suggests the definition of “(c) competence” as it relates to “fit and proper” for IT staff, vendors and contractors authorised to access the financial institution’s systems be more generally defined as “confirmed competent as determined by management” as the competence may not relate to a qualification but could be certification based, or even vendor based training internal to the vendor that is offering an IT solution.	Noted. Included certification under competence.
66	FirstRand	fit and proper’	Is this in reference to FAIS for instance. If so, there may be confusion with the fit and proper requirements that are related to IT personnel. To avoid confusion in respect of fit and proper requirements in other financial sector legislation, please clarify that the “experience and expertise” and “qualifications” is specifically IT related.	The Joint Standard relates to IT Risk. Honesty and integrity goes beyond the scope of IT Risk and competency is assessment based on the nature of the work that the person is required to do.
67	FirstRand	‘senior management’	The term ‘senior management” in this standard contains some elements of the definition of “key person” in the Financial Sector Regulation Act but is not fully aligned. Is the intention for “senior management” to be considered as “key persons” under the FSR Act? If so, to ensure alignment to the enabling legislation, we recommend linking the definition to the FSR Act definition, but contextualising which category of the FSR Act definition is relevant for this standard. Please note the above, implies throughout the standard.	Senior management is a concept is that is widely understood in banking regulations. The definition of key person has a wider scope than senior management for the purposes of this Standard. Also see response to the latter part of comment 57.
68	FirstRand	General	Suggest review of alphabetical ordering of definitions as some are out of place.	Noted. The Standard has been re-ordered.
69	JSE		No comment	Noted
70	Ubank		No comment	Noted
71	J Hayden		No comment	Noted
72	Maitland		No comment	Noted
73	Assupol Group		Seeking clarity on the definition of material incident and the reporting thereof ‘*material incident’ refers to a disruption of a business activity, process or function which has, or is likely to have, a severe and* ***widespread impact on the financial institution’s operations, services to its customers****, or the broader financial system and economy;* The clarity required relates to whether the words “……*widespread impact on financial institution’s operations, services to customers….”* exclude day to day incidents that are experienced and resolved within a short period of time as part of operations. Our reading is that it refers to: “*Significant events that demand a response beyond the routine resulting from uncontrolled developments that could lead to disaster recovery/or prompt for a full BCP*.”	As long as the event is classified as material it must be reported. Not all material incidents will result in a full BCP.
74	SAIA	“governing body” as defined in section 1 of the Act	In consideration of group structures with multiple financial institutions and financial service providers, there is a central overarching governing body as well as governing bodies for each institution. Where the Joint Standard sets out roles, responsibilities, and requirements for a “governing body”, please could the Authorities provide clarification as to which governing body is being referred to?	The FSR Act defines governing body and in this sense it means the ultimate governing body.

No	Commentator	Paragraph of the Standard	Comment	Responses
75	SAIS	Section 3: Definitions and interpretation. Definition of Financial Institution	As part of the definition of a financial institution, "a market infrastructure registered in terms of the Financial Markets Act 2012 (Act No. 19 of 2012); a discretionary FSP as contemplated in the Code of Conduct for Administrative and Discretionary FSPs, 2003; and an administrative FSP as contemplated in the Code of Conduct for Administrative and Discretionary FSPs, 2003, published in terms of the FAIS Act". As such, the SAIS is of the opinion that this standard will not be applicable to all authorised users. However, it is important to note that the majority of authorised users are also FSPs and there will be a direct impact on these authorised users. The SAIS has therefore provided comment, in relation to this standard, from this perspective and with this context in mind.	This Standard is only applicable to the financial institutions as defined.
76	HBZ Bank	3.1	Noted.	Noted
77	ECIC	3.1	Should definitions related cloud services and cybersecurity not be included given their current relevance in the IT risk context.	The outsourcing paragraph relating to cloud has been removed from the Joint Standard. Outsourcing will be covered in a separate Joint Standard and financial sector law will apply until such time as the Joint Standard is finalised.
78	GENERIC Insurance Company		No comment	Noted.
79	FirstRand	3.1	Consider including definitions for the terms 'cloud/cloud computing', 'outsourcing', and 'offshoring' as contained in the relevant directives of the PA because these terms are sometimes interpreted in different ways. Material Incident (3.1) BASA suggests renaming this definition to 'Material IT Incident' and to add the words 'system failure' to the definition as follows: "*refers to a system failure resulting in the, disruption of …".*	See response to comment 77. Disagree, the definition is suitable and broad enough to capture material incident. Not all material incidents are a result of a systems failure.
80	Hollard	3.1	'material incident' –Does material incident have a timeframe associated?	The definition of material incident does not have an associated timeframe but relies on impact to the business of the financial institution. The Authorities will determine the form and manner for the reporting of material incidents and areas related to this Joint Standard.
81	Masthead	S3.1	As the definition of 'fit and proper' currently reads, "fit and proper" is a "person complying …". With respect, this does not make sense. We suggest that the words/phrase being defined should be "fit and proper person". In our view, that would make this definition as well as other sentences and context where this definition/phrase is used, read correctly.	Disagree, when substituting the definition of "fit and proper" where the term is used, the definition makes sense in the context.
82	Masthead	S3.1	The definitions sets out the following definition of F&P: *'fit and proper requirements' means requirements relating to —* *(a) honesty and integrity;* *(b) good standing;* *(c) competence, including —* *(i) experience or expertise;* *(ii) qualifications; and* *(iii) technical knowledge of IT solutions and IT risks as the case may be;* This requirement is not listed in the definition of fit and proper provided in Board Notice 194 and may lead to inconsistencies and challenges to compliance. In our view, rather than trying to include a competence of technical knowledge of IT solutions and IT risks (which attaches to an individual or person, per the current definition in this Joint Standard), we propose that (iii) technical knowledge of IT solutions and IT risks as the case may be, is incorporated as a F&P operational requirement of the Category (CAT II & CAT III) business/FSP, under Board Notice 194.	Noted, the definition of fit and proper requirements have been amended to consider this comment. The requirements for technical knowledge has been removed from the definition and inserted in paragraph 7.3(i)(ii) In terms of the comment on vagueness, the Authorities advise that the requirements of the Standard must be implemented in accordance with the nature, size and complexity of a financial institution as well as the requirements of the position that is being considered.

No	Commentator	Paragraph of the Standard	Comment	Responses
			It is further our view that the requirement of (iii) technical knowledge of IT solutions and IT risks as the case may be, is very vague and may lead to challenges for FSPs who are required to apply this standard.	
83	SAHL		No comment	Noted.
84	Masthead	S3.1 and S7.3(i)	The definition of 'fit and proper requirements' in this draft includes (iii) technical knowledge of IT solutions and IT risks. This definition is specifically used in Section 7.3(i), (i)(ii) and in this section is applicable to staff, vendors and contractors, who are authorised to access the financial institution's systems, requiring that they must be fit and proper and be contractually required to protect sensitive or confidential information. It is unclear from the definition if this requirement applies specifically and only to KIs and Representatives who are staff, vendors or contractors as per the Board Notice 194 scope or, if in this instance, these fit and proper requirements apply to all staff, vendors and contractors, regardless of their authorised status as KI or representative. In our view, the proposed change to the definition, as explained in our comment on section 3.1 above, will address this uncertainty. Further, it is our view that the scope of this new requirement is not clear as we are unsure how the new requirement of (iii) technical knowledge of IT solutions and IT risks as the case may be, will be tested, measured or verified by the FSP.	Disagree. Please see comment under item 82 above. Staff, vendors and contractors, who are authorised to access the financial institution's systems, must comply with the fit and proper requirements imposed on such persons by the relevant sectoral law. Accordingly, this requirement is only applicable insofar as it is a requirement, in terms of the sectoral law, to comply with fit and proper requirements, i.e. financial services providers, their key individuals and their representatives.
85	BASA	Recovery Time	"Objective" instead of "Object".	Noted. The definition has been updated accordingly.
86	BASA	RPO (3.1)	BASA suggests including the words or "*system disruption*;" after the words 'should a disaster'	Noted. The standard has been amended accordingly.
		4. Application		
87	SAIA	This Standard applies to financial institutions as defined.	a) Please confirm how the Joint Standard relates to insurance groups and banking group standards that drive consistent and single frameworks. It is recommended that recognition of this current status be afforded. b) The intended scope of application contained in the Statement of Need differs slightly from the Annexure C definition of a "financial institution". The Statement of Need includes an insurance group (insurer) but Annexure C omits this reference. It is acknowledged, and in consideration of the Prudential Standard GOG (Governance and Operational Standard for Insurance Groups) requirements, that within insurance groups, although group-wide policies and frameworks apply as minimum standards at the controlling company level, each entity within an insurance group may have more granular frameworks and standards in place commensurate to its business. These may include entities located outside of South Africa who may also be subject to different regulatory requirements. Accordingly, the Authorities are requested to please clarify their position on the inclusion of insurance groups within the scope of application of the Joint Standard.	a) The Joint Standard has been amended to apply to insurance groups. b) All documents have been aligned.
88	SAIA	This Standard sets out the requirements for sound practices and processes of IT risk management.	There is a view that the proposed Joint Standard is more prescriptive than outcomes-based. The Authorities are requested to consider adopting a better balance between rules and principles to support a more outcomes and risk-based supervisory approach.	The Authorities is of the view that the joint Standard is to the extent necessary principle based however, there are minimum requirements in some areas that need to be prescribed via rules.
89	HBZ Bank	4.1	Noted	Noted.
90	ASISA	4.1	There is a discrepancy between paragraph 5.1 of the Statement of the need for, intended operation and expected impact of the proposed Joint Standard (Statement of Need) and paragraph 4.1 of the Draft Joint Standard. The reference to insurance groups in paragraph 5.1 of the Statement of Need causes uncertainty as to whether the requirements are intended to apply to all companies that form part of an insurance	Refer to response as per comment number 87.

No	Commentator	Paragraph of the Standard	Comment	Responses
			group. An insurance group is designated (not licensed) in terms of the Insurance Act for the purpose of facilitating the prudential supervision of an insurer. It is thus presumed that the requirements of the Joint Standard will therefore not be applicable to all companies in an insurance group but only to those companies that are financial institutions as per the definition contained in the Draft Joint Standard. The Authorities' confirmation in this regard will be appreciated.	
91	BASA	4.1	BASA notes that the provision determines that "The Standard will apply to financial institutions as defined". Please see our note regarding the definition of "financial institution" above. However, one financial institution can be licensed/authorised to act in various capacities detailed in the Standard, for example an entity that is licensed as a Bank or Insurer can also be a Financial Services Provider. BASA recommends that clarity be provided on the impact of the Standard in relation to financial institutions that are licensed for more than one activity and whether the requirements of the Standard should be adhered to in respect of each authorisation.	The Authorities is of the view that if the financial institution is licensed for more than one activity, each entity licensed must comply based on the size nature and complexity irrespective of where controls have been defined from. The minimum requirements are the same for the various financial institutions and the financial institution must apply the principles based on the nature, scale and complexity. Each financial institution captured by this Joint Standard must be able to prove compliance with the requirements on institution-specific risk whether it is captured at an institution level or at a group level.
92	FirstRand	4.1	We note that the Standard applies to the Banking entity, as well as to managers of CIS, insurers, a market infrastructure and to discretionary and administrative FSPs (per the definition of a "financial institution". Does the Draft Standard not apply to: • Category 1 only FAIS FSPs? (in other word the existing FAIS General Code of Conduct standards pertaining to IT risk management will continue to apply to a category 1 FSP?) Non-banking investment holding entities in a conglomerate?	The joint Standard is only applicable to the institution defined as per paragraph 3.1. It does not apply to Category 1 FSPs. The financial conglomerate will apply this requirement on a consolidated basis in terms of the bank controlling company and the insurance group.
93	FirstRand	4.2	FirstRand recommends that this be established as a minimum standard for financial institutions as IT Risk increases and modus operandi changes. Financial Institutions must be agile to adapt where necessary to these new threats.	Noted. The standard has been amended to reflect that it contains minimum requirements.
94	HBZ Bank	4.2	Understood the purpose and rationale for these regulations	Noted.
95	HBZ Bank	4.3	Noted	Noted.
96	SAIS	Paragraph 4.3	As stated in the draft, "The requirements of this Standard must be implemented in accordance with the nature, size and complexity of a financial institution". Whilst this section may give institutions flexibility in terms of compliance, it may be difficult to determine the extent of compliance required. The Standards could outline the minimum, basic cost-effective requirements for small institutions. It must be ensured that the cost of the additional layers of regulation does not become a barrier to entry, thereby excluding many role players.	The Joint Standard captures the minimum requirements for IT Risk and the Objective Box and paragraph 4.5 has been amended to communicate this approach.
97	PSG Konsult		No comments.	Noted.
98	BASA	4.3	BASA seeks clarity for tier 2 Banks where a tier 2 Bank does not have the necessary resources and or budget capacity to implement all the requirements as set out in the Joint Standard. The provision determines that "*The requirements of this Standard must be implemented in accordance with the nature, size and complexity of a financial institution*." It is our understating that this provision may lead to inconsistent application unless objective criteria or the Authorities' views on objective criteria is provided. As such, we are concerned that this may seem a contradiction in terms. A standard defines the minimum expected; and is also legally enforceable. We therefore recommend that the expectations must be clear and not open to interpretation. If different expectations are desired for different tiers this must be explicitly delineated in the document.	The Joint Standard sets out the minimum requirements for IT Risk and applies to banks and controlling companies on a solo and consolidated basis. No changes were made, as paragraph 4.3 provides clarity on implementation. As banks increase their IT Risk, the minimum requirements must be adapted and evolve to ensure that the principles of the Standard are followed.
99	Just SA	4.3	The IT Risk Joint Standard is very comprehensive, however may be impractical from a cost, resources and capacity perspective for smaller institutions to implement all the required standards based on the nature and size of these organisations.	Refer to response to comment 98.
100	GenRe		No comment	Noted.
101	HBZ Bank	4.4	No Comments	Noted.

No	Commentator	Paragraph of the Standard	Comment	Responses
102	FirstRand	4.4	FirstRand recommends that we add "*and in conjunction with relevant financial sector directives and guidance notes from the Prudential Authority*" For example, directive D2-of-2019 on the reporting of material information technology and-or cyber incidents, amongst others.	Noted, this Standard applies in addition to other relevant laws.
103	Ubank		No comment	Noted.
104	J Hayden		No comment	Noted.
105	Maitland		No comment	Noted.
106	SAHL		No comment	Noted.
107	BNP Paribus		No comment	Noted.
108	BASA	4.4	Non-financial sector laws such as the Cybercrimes Act and POPI are explicitly impactful throughout the Standard – it is recommended that the Authority extends the requirement for contextual legislative application to further that financial sector legislative instruments and include consumer protection related regulatory instruments. From the objective of the standard, it is further derived that an objective thereof relates to consumer protection.	Noted, this Standard applies in addition to other relevant laws.
109		No Concerns. Sections 3 & 4 are swapped in the Draft Standard and this review Template.	No Concerns. Sections 3 & 4 are swapped in the Draft Standard and this review Template.	Noted.
110	Maynard Bester (ISACA member)		No comment.	Noted.
111	BDO		No comment	Noted.
112	FEMA		No comment	Noted.
113	ECIC		No comment	Noted.
114	GENERIC Insurance Company		No comment	Noted.
		5. Roles and responsibilities		
115	HBZ Bank	5.1	Noted	Noted.
116	FirstRand	5.1	It is in the FirstRand view that accountability and responsibility be separated to support the practical implementation of these Standards. Accordingly, we propose the following: a) 5.1 be amended to remove the word "responsible" and be replaced with "*accountable*". b) FirstRand requests an additional section under this heading, allowing the governing body and senior management to delegate the responsibility to meet the requirements of the Standard to appropriate operational persons/team. The governing body and senior management will continue to be accountable for the actions of the delegates. Refer also to FirstRand's comment in Section 3, No 2 above.	a) The Authorities hold the board ultimately responsible for ensuring compliance with this standard. b) The delegation of responsibility is an internal matter.
117	FirstRand	5.2	Senior management has not been adequately defined. Given the various flat and hierarchical structures in most financial institutions, senior management is often present/evident in many layers of the organisation. If this is a board mandated responsibility, it must be expressly mentioned. FirstRand considers IT Risk to be a subset of operational risk, and hence does not require separate frameworks or standards for IT Risk. The operational risk standards and policies are all applicable to and is fully adopted by IT Risk. FirstRand therefore recommends that the statement in the standard be amended to "*must ensure that there are sound and robust risk management frameworks which are applicable to IT risk*…". Refer to FirstRand's comments in Section 7 below, No 1. Similarly, and particularly in a digital age, IT strategy cannot be separated from overall business strategy and it is considered unnecessary to have a separate, discrete strategy for IT. FirstRand suggests that this statement should be amended to "... *framework and must ensure that IT objectives are aligned and integrated with the organisation's strategy*".	The Authorities are of the view that the current definition is sufficient. Without further details on the inadequacy of the definition level we are unable to expand the definition. In addition, paragraph 5.3 – states that roles and responsibilities must be clearly defined. Noted, however, the Authorities recognised the maturity is at different level for organisation, the principle is to ensure alignment of both IT and business. The Authorities are of the view that each business unit must have its own strategy and objectives aligned to the overall organisation strategy.

No	Commentator	Paragraph of the Standard	Comment	Responses
118	J Hayden	5.2	The governing body, together with senior management, must ensure that a sound and robust IT governance and risk management framework such as COBIT is established and maintained.	The Authorities do not prescribe a preferred framework as this choice must be made by the relevant financial institution. The Authorities however, expect that the requirements of this standard are met when applying a particular framework.
119	HBZ Bank	5.2	Noted	Noted.
120	BASA	5.2 Capitec 2nd	A dominant trend is for IT risk management to be addressed principally by applying over-arching risk management frameworks augmented with any additional IT elements as required, and it is considered undesirable to have a discrete, stand-alone risk management framework for IT. BASA is concerned that this is the intent of this paragraph and further suggests the amended wording as below. Similarly, and particularly in a digital age, IT strategy cannot be separated from overall business strategy and it is considered undesirable to have a separate, discrete strategy for IT. BASA suggests the following wording: '*The governing body, ~~together with senior management~~* **together with Key Persons**, *must ~~ensure that a sound and robust IT risk management framework and IT strategy is established and maintained~~ ensure that the organisation's risk management frameworks specifically address IT risk management.'*	The Authorities note the recommendation. However, paragraph 5.2 states that the governing body together with senior management must ensure that a sound and robust IT risk management framework and IT strategy is established and maintained. It does not require the IT risk management framework or strategy to be severed from the overall strategy and risk management of the financial institution.
121	GenRe	5.3	"…as well as committees established for the purpose of exercising oversight of IT risks." The responsibilities of the governing body are very wide and may not be practical.	Paragraph 5.3 clearly states the duty of the board to define the role of senior management, control functions and committees in IT risk management.
122	HBZ Bank	5.3	Noted	Noted.
123	J Hayden	5.4	The governing body, together with senior management, must ensure that an IT strategy is established and executed.	Noted. The Authorities have amended section 5.3 to cater for the execution role of management.
124	SAIA	The governing body is ultimately responsible for ensuring that the financial institution complies with the requirements as set out in this Standard.	The Authorities are requested to clarify whether this requirement is intended for a governing body at each entity level or whether the governing body at a group level will suffice.	The standard applies to the financial institution as per the definition. If it is a controlling company of a bank or an insurance group, the board means the board of the controlling company.
125	FirstRand	General	The governing body should exercise an oversight function, including monitoring effectiveness of the function. Responsibilities for design and implementation and internal controls and risk management should rest with the relevant senior management functions. Refer also to FirstRand's comment in Section 3, No 2 above.	Noted. The governing body needs to ensure that an effective risk management framework and strategy is implement. After all, these are board approved frameworks.

No	Commentator	Paragraph of the Standard	Comment	Responses
126	BASA	General	BASA would appreciate guidance on which line of defence is responsible for which control in this Standard. Please refer to our comments herein above at 3.1 concerning the definition of 'senior management'.	The Authorities are of the view that lines of defence are defined by the respective financial institution to ensure separation of roles and independence. The lines of defence are not defined by this joint Standard, but by other financial sector law as stated in paragraph 4.6. The financial institutions when detailing responsibilities must align such with the applicable lines of defence in terms of their respective governance and risk management frameworks.
127	SAIS		No comments.	Noted
128	PSG Konsult		No comments.	Noted
129	Assupol Group		No comments	Noted
130	Maynard Bester (ISACA member)		No comment.	Noted
131	BDO		No comment	Noted
132	FEMA		No comment	Noted
133	ASISA		No comment	Noted
134	ECIC		No comment	Noted
135	GENERIC Insurance Company		No comment	Noted
136	JSE		No comment	Noted
137	Ubank		No comment	Noted
138	Maitland		No comment	Noted
139	SAHL		No comment	Noted
140	BNP Paribus		No comment	Noted
6. IT Strategy				
141	HBZ Bank	6.1	Noted	Noted.
142	BASA	6.1	With reference to BASA's comments at 5.2 above, a separate, discrete IT strategy is not ideal, therefore, BASA recommends the following amended wording *"A financial institution must ensure that its strategy,* **and specifically IT strategic objectives incorporated therein, are** *approved by the governing body and* **that the IT specific strategic objectives** *are aligned to the overall business strategy."*	Noted, however, the Authorities recognised the maturity is at different level for organisations, the principle is to ensure alignment of both IT and business. The Joint Standard does not prohibit the strategy or risk management related to IT to form part of the enterprise risk management system but that it must be easily identifiable. However, the Authorities are of the view that each business unit must have its own strategy and objectives aligned to the overall organisation strategy.
143	JSE	6.2	Suggested grammatical amendment: The IT strategy of a financial institution must be reviewed regularly, but at least annually.	Noted, changes have been made
144	HBZ Bank	6.2	Suggest the review period to be increased to 3 years so as to provide the Governing Body sufficient information to assess the efficacy of the strategy	The requirement of the Authorities is that the strategy be reviewed regularly but at least on an annual basis as a strategy needs to be adapted as market conditions, internal conditions and other risk

No	Commentator	Paragraph of the Standard	Comment	Responses
				change and evolved. A strategy is dynamic in nature and requires regular review.
145	Masthead	S6.2	s6.2 - Since the IT strategy of a financial institution must be reviewed at least annually, we do not see the need to include the word “regularly”.	Annually is the minimum review requirement, regularly speaks to where events occur and it necessitates a review of the IT strategy.
146	BASA	6.3.a	BASA notes that the terms "action plans" is not defined in the Standard and suggest that it may be better described given that the Standard mandates that these ‘action plans’ are established and reviewed at least quarterly. If the term ‘action plans’ does not differ substantially from the meaning of "IT projects and programs", as included in the definitions section, then BASA suggests that that term be used instead of ‘action plans’. BASA seeks clarity on whether quarterly reporting in terms of progress against targets equates to the review of the actions and in addition we suggest that six-monthly review may be more appropriate.	The Authorities are of the view that there is no need to define action plans. Action plans may involve IT projects and programmes but could also involve recruitment, human resource interventions and other initiatives to deliver on the IT strategy. The action plans review feed into the overall review of the strategy therefore the quarterly review is considered appropriate to track the progress in terms of the overall strategy review, which must be conducted at least on an annual basis.
147	AVBOB	6.3.a.	“…Regularly but at least quarterly...” is very stringent as part of a standard. Quarterly would seem like a reasonable review period and certainly one that every institution should aspire to, but not a minimum. Would prefer minimum to be annually.	The action plans review feed into the overall review of the strategy therefore the quarterly review is considered appropriate to track the progress in terms of the overall strategy review, which must be conducted at least on an annual basis.
148	Masthead	S6.3(a)	*s6.3(a) - … establish a set of action plans that contain measures to be taken in order to achieve the objective of its IT strategy. The action plans must be communicated to all relevant staff and must be reviewed regularly, but at least on a quarterly basis, to ensure their relevance and appropriateness;* A quarterly review requirement has a significant cost and resource impact and in terms of frequency of monitoring, which is more than what is prescribed for Conflict of Interest or Fit and Proper under the FAIS Act. In our view, this requirement is too onerous. FSPs should be allowed to apply a proportionate and risk-based approach which is suitable to their organisation size and nature, as provided for in section 4.3 of this Joint Standard. The prescription of a quarterly review is very rules-based and, in our view, detracts from the regulatory intent of moving to more principle-based regulation.	Disagree. Due to the evolving nature and serious impact of IT risks, in order to ensure relevance and appropriateness, the Authorities believe quarterly reviews of the action plans are appropriate.
149	HBZ Bank	6.3 a	Suggest the action plan review to be annually rather than quarterly in order to give sufficient time to assess the results	The action plans review feed into the overall review of the strategy therefore the quarterly review is considered appropriate to track the progress in terms of the overall strategy review.
150	Maitland	6.3 (a)	We submit that the frequency of the reviews should be based on the nature and size of the financial institution’s operations, as quarterly reviews may otherwise prove onerous.	Disagree. Due to the evolving nature and impact of IT risks, in order to ensure relevance and appropriateness, the Authorities believe quarterly reviews of the action plans are appropriate.
151	GenRe	6.3 (a)	Strategic action plans are long-term plans and therefore the need for a quarterly review may be considered onerous.	The action plans review feed into the overall review of the strategy therefore the quarterly review is considered appropriate to track the progress in terms of the overall strategy review, which must be conducted at least on an annual basis.
152	FirstRand	6.3 (a)	FirstRand’s comments in section 5, No 3 has reference. FirstRand recommends removal of the words “…of its IT strategy.” in the first sentence. Frequency of review of progress against IT objectives will vary amongst institutions; hence FirstRand recommends that the second sentence be amended to “*…reviewed regularly in accordance with the financial institutions internal processes to ensure relevance and appropriateness*”.	The Authorities require an identifiable IT strategy, kindly refer to the response to comment 142. The Authorities are of the view that attaching timeline to this principle will ensure compliance and it would be adequately assessed across the sector. In addition, the quarterly requirement fits well into the requirement to review the overall strategy on an annual basis.
153	HBZ Bank	6.3 b	Noted	Noted.
154	FirstRand	6.3 (b)	FirstRand’s comments in section 5, No 3 has reference. FirstRand recommends replacing the words “IT strategy” with “*IT objectives*”.	Refer to response provided to comment 142.
155	AVBOB	6.3b	Who does the monitoring and measuring of the effectiveness of the IT strategy – is it a 1st line or a 2nd line function or a combined assurance type approach? How would 2nd line determine effectiveness?	Section 5.3 provide a guidance on defining roles and responsibilities including oversight functions. The Authorities are of the view that compliance to this principle includes but is not limited to ensuring monitoring and measuring the effectiveness of the controls defined.

No	Commentator	Paragraph of the Standard	Comment	Responses
156	J Hayden	6.3 (b)	establish processes to monitor, measure and report to the governing body on the performance, delivery, and effectiveness of the IT strategy	Noted. The Authorities are of the view that the provisions are sufficient.
157	Brightrock	6.3(C)	Please provide clarity on the form and manner in which reporting to Authorities are required.	The form and manner will be determined or specified by the Authorities once the Joint Standard is finalised.
158	HBZ Bank	6.3 c	Noted	
159	ASISA	6.3(c)	It is not understood why a financial institution that is only being supervised by one financial sector regulator (a responsible authority as defined in the Financial Sector Regulation Act) should inform both the Authorities when there is a deviation from the IT strategy that may be a contravention. It is also unclear why contraventions of any other legal requirements which could potentially include contractual arrangements should be reported. A financial institution should only be required to inform the responsible authority for a financial sector law of contraventions of financial sector laws. It is proposed that paragraph 6.3(c) of the Joint Standard should be amended accordingly. --- *A financial institution must ensure that the ~~Authorities are~~ <u>responsible authority is</u> informed when there is a deviation from the IT strategy that may contravene this Standard or any ~~other legal~~ requirements relating to IT risk management <u>contained in financial sector laws.</u>*	Noted, the Joint Standard has been amended accordingly.
160	FirstRand	6.3 (c)	It is the FirstRand's view that this requirement may lead to a flood of reporting to the FSCA. Taking a risk based approached, it is FirstRand's recommendation that only material deviations from the IT strategy that may contravene this Standard be communicated to the Authorities. We would welcome an opportunity to discuss the elements of materiality that would warrant reporting. Clarity is also sought on the following: a) What is the purpose of the reporting? b) When must the deviation be reported i.e. before such deviation is considered by the Financial Institution (FI) or before implementation? c) Will reporting mitigate the risk of regulatory sanctions under this Standard and/or applicable financial sector laws? d) Will this report be kept confidential? It is our view that this type of information in the public domain may cause undue concerns and panic. This requirement must also be clarified in terms of section 19(2)(a) of POPIA which requires the Responsible Party to identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control. The suggestion is to align the IT Risk framework with the Information Regulator requirements as Financial Institutions will also be considered as Responsible Parties under POPIA.	The deviation only relates to the potential that the Joint Standard may be contravened. It is not necessary to stipulate that it is material or not – the test is whether it will lead to a possible contravention of the Joint Standard or other legal requirements relating to IT risk. The form and manner for reporting will be consulted on prior to finalisation. The financial institution must comply with POPIA but has to report to the responsible authority in the form and manner determined or specified.
161	Ubank		No comment	Noted.
162	Maitland	6.3 (c)	We suggest that the wording be amended as follows: ensure that the *<u>relevant Authority/ies, which supervise/s the financial institution,</u>* ~~Authorities~~ *<u>is/are</u>* informed when there is a deviation from the IT strategy that may contravene this Standard or any other legal requirements relating to IT risk management.	The Joint Standard has been amended to require reporting to the responsible authority for the financial sector law in terms of which the financial institution is licensed or registered.
163	Masthead	S6.3(c)	*s6.3(c) ensure that the Authorities are informed when there is a deviation from the IT strategy that may contravene this Standard or any other legal requirements relating to IT risk management.* This section introduces a self-reporting requirement to the Financial Sector Conduct Authority (FSCA) and the Prudential Authority. The requirement is worded extremely broadly and, in our view, no materiality measure is applied. This implies that all non-compliance must be reported, without regard to materiality. It is our view that a measure for materiality should be introduced, similar to irregularity reporting limits to ensure that	Disagree. Non-compliance with any provision of this Standard, regardless of materiality, is a contravention of legal requirements. The requirement is therefore that any deviation must be reported. In order to address the concern, wording that "within a reasonable time", has been insert into the provision.

No	Commentator	Paragraph of the Standard	Comment	Responses
			the Regulator is notified of risks or significant issues, rather than all incidents. This section is also not clear in terms of prescribing a timeframe. Further to the comments above, we question the practical application and usefulness of this provision – if the financial institution needs to develop an IT strategy that is aligned to this Joint Standard, it seems improbable that it will self-report that it is deviating from this Standard.	Disagree. The rationale for the Standard, as well as the risks associated with IT, is set out in the Statement of Need. Should a financial institution fail to report deviations from this Standard, which could lead to the risks materialising, the Authorities could take regulatory action against such an institution.
164	SAHL	6.3 (c)	Please elaborate on the type of actions to be reported to the Authorities that will fall within the ambit of a deviation from the IT Strategy as IT is regularly updating.	Refer to response provided to comments 157 and 160.
165	AVBOB	6.3c	What deviations would contravene this standard? What triggers would activate notification to the authority? It appears that almost anything could be construed as "may contravene" this standard. Is the intention that almost all events should be reported or only material exceptions? Examples would be useful.	Refer to response provided to comments157 and 160.
166	AVBOB	6.3.c.	Assuming that there is already a requirement to report contraventions of legal requirements or standards with reasons, it is unclear why a deviation from IT strategy that "may" result in a contravention is specified explicitly, and could result in a high reporting burden as "may" is not a well-defined criteria.	Refer to response provided to comments 157 and 160.
167	BASA	6.3 (c)	Clear criteria for reporting changes in IT Strategy should be set as having it generic may result in an onerous requirement (being too wide). For example, it makes sense to report a change in IT Strategy from on-prem solutions to cloud solutions, but it would not make sense to report a change in strategy from AWS to Azure (change ins service provider). BASA therefore suggests the following amended wording: "ensure that the *appropriate Regulatory Authorities* are informed when there is a *materia*l deviation". This requirement must also be clarified in terms of section 19(2)(a) of POPIA which requires the Responsible Party to identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control. The suggestion is to align the IT Risk framework with the Information Regulator requirements as Financial Institutions will also be considered as Responsible Parties under POPIA.	Refer to response provided to comments 157 and 160.
168	GenRe	6.3 (c)	"ensure that the Authorities are informed when there is a deviation from the IT strategy that may contravene this Standard or any other legal requirements relating to IT risk management." This requirement may be considered onerous.	Refer to response provided to comments 157 and 160.
169	Telesure	6.3 (c)	Clarity is needed on the manner and form in which a financial institution should communicate a deviation from its IT strategy. And when would a deviation from an IT strategy need to be reported. Will this be limited to material deviations only?	Refer to response provided to comments 157 and 160.
170	SAIA	A financial institution must ensure that its IT strategy is approved by the governing body and aligned with its overall business strategy	The Authorities are requested to clarify whether this requirement is intended for a governing body at each entity level or whether the governing body at a group level will suffice.	For bank controlling companies and insurance group, the requirements must be applied on a consolidated basis.
171	SAIA	A financial institution must ensure that the Authorities are informed when there is a deviation from the IT strategy that may contravene this Standard or any other legal requirements relating to IT risk management.	The Authorities are requested to confirm whether:- a) A prescribed format for reporting such deviations to the Authorities, be provided. b) The Authorities will prescribe timeframes for such reporting.	There is no time frame, the Authorities requires reporting as and when there is a change. The form, manner and period for reporting will be determined or specified by the Authorities.

No	Commentator	Paragraph of the Standard	Comment	Responses
172	BNP Paribus		No comment	Noted
173	SAIS		No comments.	Noted
174	PSG Konsult		No comments.	Noted
177	Assupol Group		No comments.	Noted
178	Maynard Bester (ISACA member)		No comment.	Noted
179	BDO		No comment	Noted
180	FEMA		No comment	Noted
181	ECIC		No comment	Noted
182	GENERIC Insurance Company		No comment	Noted
7. IT risk management framework				
183	HBZ	7.1	Noted	Noted.
184	J Hayden	7.1	A financial institution must establish an IT risk management framework such as COBIT to manage IT risks in a systematic and consistent manner.	The Authorities do not prescribe a preferred framework as this choice must be made by the relevant financial institution. The Authorities, however, expect that the requirements of this standard are met when applying a particular framework.
185	JSE	7.1	This paragraph implies that a separate or stand-alone IT risk management framework is required and does not appear to recognise an IT risk management framework within an Enterprise Risk Management framework based on an international risk management standard (ISO31000). We respectfully request that this point is clarified.	Noted. Section 7.1 has been amended to clarify that the IT Risk management framework may form a component of the ERM framework.
186	BASA	7.1	BASA refers to its comments made herein at 5.2 above, a separate, discrete IT risk management framework is not considered desirable. This could be reworded as: "*A financial institution* **must ensure that the organisation's risk management frameworks specifically address and enable effective management of IT related risks** ~~*must establish an IT risk management framework to manage IT risks in a systematic and consistent manner.*~~	Noted. Section 7.1 has been amended to clarify that the IT Risk management framework may form a component of the ERM framework.
187	HBZ	7.2	Suggest the review period to be increased to 3 years thereby providing the Governing Body sufficient information to assess the results	Annual reviews provide an opportunity for the financial institution to made amendments based on gaps or inefficiencies in the risk management framework as a result of ever-changing IT risks.
188	Hollard	7.2	An annual independent review of the overarching IT risk management policy/ framework is not practical. This policy should be independently reviewed at least every three years	The requirement is not for an independent review by external auditors. Since risk changes on a daily basis, the requirement for the framework to be reviewed at least annually is not over prescriptive.
189	Masthead	7.2	s7.2 – similar to our comments under we do not see the need to include the word "regularly".	Regularly caters for material events that necessitates an immediate amendment to the IT risk management frameworks.
189	AVBOB	7.2	Would the organisation's ERM framework be acceptable to meet this requirement or would a separate IT risk management framework be developed and approved by the Board?	The IT Risk Management framework may form part of the financial institution's Enterprise Risk Management framework or overall risk management framework, provided that the IT risk framework clearly identifiable, board-approved and reviewed regularly, but at least annually.
190	ECIC	7.3	Is the annual review of the framework not too prescriptive? For example, some policies within the ECIC are reviewed every 3 years or as and when required.	Due to the evolving nature of IT risks, in order to ensure that such risks are properly managed, the Authorities believe regularly reviewing of the IT risk management framework, with the minimum requirement being annually, is reasonable and proportionate.
191	FirstRand	7.3	FirstRand's comments in Section 5, No 3 also has reference here.	See response to comment 189 above. Please note that the words 'attributes and requirements' have been deleted from the root

No	Commentator	Paragraph of the Standard	Comment	Responses
			Many of the statements which follow in this document may be covered in different policies, standards and procedures. It is not natural that all of this should be included in an IT Risk Management Framework. Suggestion here is that we should replace with something like "*A financial institution must ensure that the following attributes and requirements are included in relevant policies, standards or procedures*:" Word "Encompass": Please consider adding the words '*or makes reference to the relevant policy or artefact*' as not all these aspects are included in the IT risk management framework but are included in other related policies/processes/standards.	paragraph of 7.3. The word 'encompass' has been substituted with 'incorporate'
192	Just SA	7.3	Based on the nature and size of an organisation, will it be sufficient for a smaller organisation to have a broader Enterprise Risk Management Framework that covers IT risks and policies or is the expectation to have a separate specific IT Risk Management Framework.	See response to comment 191. The requirement is for a financial institution to have an IT risk management framework. It is not prescribed that such a framework has to be separate. Please also refer to paragraphs 4.5 and 7.1 of the revised Joint Standard.
193	BASA	7.3	BASA suggests the following wording: "*The IT risk management framework of a financial institution must, at a minimum, encompass* **or be linked to other policies, processes, procedures and standards** *the following attributes and requirements -*	See response to comment 191.
194	JSE	7.3(a)	See general comment below in respect of the use of the term 'organisation'.	Noted. The word 'organisation' has been changed to 'financial institution'.
195	Just SA	7.3 (iv)	Is the function or department referred to in this paragraph a first line function such as the IT department or a second line Risk Management function?	The financial institution must comply with this requirement. The structure of compliance is not prescribed.
196	AVBOB	7.3a	IT standards and procedures sounds too operational for the governing body to approve.	Due to the materiality of the risk posed through IT risk, it is crucial that standards, policies and processes be approved by the board/governing body.
197	Hollard	7.3 (a)	IT policies should be reviewed during the course of the internal/ external audit review program and while standards and procedures may be considered, this should not be prescribed but left to the design of the Insurers internal control governance.	It can be done by external or internal auditors but this must be done.
198	HBZ	7.3 (all sections)	Noted	Noted.
199	FirstRand	7.3 (a)	Can 'IT' be removed from the following statement as some of the policies implemented to address the requirement may not be IT specific policies: "IT policies, standards and procedures in managing IT risks and safeguarding IT assets in the organisation"	Noted. 'IT' has been removed before 'policy' from (a) and (c).
200	Maitland	7.3 (b)	We suggest that the wording be amended as follows: the ability to detect, control and limit all major *IT risks identified*, taking into consideration the principle of proportionality;	Disagree. In the context, it is clear that reference is made to IT risks.
201	BASA	7.3.b	BASA suggests that the words "detect, control and limit" should be replaced with industry standard language, such as "identify, assess and manage".	Noted, the paragraph has been amended.
202	BASA	7.3.c	BASA seeks clarity on the reference to "independently reviewed" with regard to "policies, standards and procedures" whether this refers to it being reviewed by a relevant committee, or an internal audit function etc.	Please refer to response to comment 197.
203	Masthead	7.3(c)	*s7.3(c) IT policies, standards and procedures must be independently reviewed and updated to take into account, among others, rapid changes in the IT operating and security environment;* The implementation of a requirement of independent review comes with an added and potentially high cost impact for FSPs. We feel that, in view of the broader financial, economic and social environment, this will have a negative financial impact on these FSPs at this time. In addition, this section states that these documents must be independently reviewed *AND* updated. Does this mean that the FSP must contract an external party to make actual changes (i.e. update) to the FSP's policies etc.? In our view, the word "independently" should not attach to the word "updated". This Joint Standard already requires (in section 4.3) that financial institutions should apply a proportionate and risk-based approach which is suitable to their organisation size and nature. Therefore, it should be left to the financial institution to decide whether	Disagree. In light of the risks involved, the Authorities are of the view that independent review is appropriate. In addition, smaller institutions might not have "senior IT management" to review the framework. Paragraph 10 has been deleted. Agree. The word "independently" only attaches to "reviewed", as the requirement is currently drafted.

No	Commentator	Paragraph of the Standard	Comment	Responses
			the nature of the business requires an external and independent party to review and update its policies, standards and procedures.	
204	Maitland	7.3 (c)	This is an onerous provision and has a cost implication. We submit that the senior IT management are the subject matter experts who are best placed to review and update policies. Par 10.3 (g) contains the requirement that the review of the information security framework must be subject to independent audit assessments. The requirement in par 7.3(c) relating to independent review is a duplication of the requirement in par 10.3 (g). We suggest that the wording be amended as follows: IT policies, standards and procedures must be ~~independently~~ reviewed and updated to take into account, among others, rapid changes in the IT operating and security environment	Disagree. In light of the risks involved, the Authorities are of the view that independent review is appropriate. In addition, smaller institutions might not have "senior IT management" to review the framework. Paragraph 10 has been deleted.
205	JSE	7.3(c)	It is not clear what is meant by 'independently reviewed'. Is it the Authorities' intention that the review should be conducted by an independent third party or would a review conducted by the financial institutions' internal audit function suffice? In addition the minimum cadence or frequency of review should be stipulated.	Refer to response to comment 197.
206	FirstRand	7.3 (c)	It is mentioned that IT Policies etc. should be "independently reviewed"? Need clarity on what independence is sought here. Can 'independent review" include review by Internal Audit? In addition, there seems to be two activities contained in this statement, one being an independent review and the second being updating of the documents. FirstRand suggests separating these two because including the "independent" party in the update process can be seeing as them thereby compromising their independence under the "review" activity. Section 7 contains attributes/requirements for an IT Risk management Framework. To this end, the suggestion is to amend this statement as follows "Include internally defined frequencies for IT policy, standard and procedure reviews, and process to ensure interim updates to take into account, amongst others, rapid changes in the IT operating and security environment". FirstRand suggests that the term 'IT' be removed from this requirement/attribute as some of the policies implemented to address the requirement may not be IT specific policies.	Noted. See response to comments 197 and 199. 'Review' and 'update' has been separated in 7.3(c)
207	AC&E	7.3 c	"IT policies, standards and procedures must be independently reviewed and updated to take into account, among others, rapid changes in the IT operating and security environment" QUESTION: Would this independent review need to be conducted by an external company (incurring cost) or would the review process be accepted as part of annual audit processes, given the nature and complexities of IT this may require its own separate review process to be setup to ensure that all requirements are being met and adhered to.	Please refer to response to comment 197 above.
208	Brightrock	7.3(C)	Please provide clarity on "independently reviewed", and what assurance providers would meet this requirement. For example, Internal Audit, Compliance, etc?	Refer to response to 197 above.
209	ASISA	7(3)(c)	It is presumed that the required independent review may be performed by an internal control function as referred to in paragraph 16.1 of the Draft Joint Standard. The cost of an external review independent of the financial institution would be unreasonable. Paragraph 7.3(c) should be amended for the sake of clarity. --- *The IT risk management framework of a financial institution must, at a minimum, encompass the following attributes and requirements –* *(c) IT policies, standards and procedures must be independently reviewed by an internal control function as referred to in paragraph 16.1 of this Standard and updated to take into account, among others, rapid changes in the IT operating and security environment.*	Noted. Independent review has been defined in the Joint Standard as follows: 'independent review' may be conducted by internal or external audit or an independent control function;
210	AVBOB	7.3c	The paragraph requires independent review – would this be a second line function or a third line or a combined assurance approach? Please clarify the intention of the meaning of independent review?	Noted, see response to comment 209.
211	AVBOB	7.3d i	Please clarify how it is envisaged that this will this be overseen – is the risk management department, combined assurance, external auditors, independent expert? is it oversee or ensure that the ICT risk management programme is developed etc	The Joint Standard is not prescriptive on the approach. It depends on the organisational structure of the financial institution.

No	Commentator	Paragraph of the Standard	Comment	Responses
212	BASA	7.3 (d)(i)	The governing body should exercise an oversight function, including monitoring effectiveness of the function. The governing body is not accountable for implementation. Responsibilities for design and implementation and internal controls and risk management should rest with the relevant senior management functions. Governing bodies may still have overall oversight or accountability, but consideration should be given to allowing for such delegations where reference is made to specific compliance obligations (apart from the governing body's obligation to have oversight and ultimate accountability).	Noted. Paragraph 5.3 defines the roles of the responsibilities of governing body. 7.3(d) does not preclude any delegations.
213	AVBOB	7.3d ii	What is deemed to be "adequate" governance – should this be a second line confirmation or third line or external auditors or an independent expert.	Adequate is relative to the institution's nature scale and complexity. The governing body will be in a position to satisfy themselves that the internal governance is adequate.
214	AVBOB	7.3d iv	For the implementation, is this envisaged to the first line IT department? For enforcement, can this be allocated to the Risk Management Department whose resource(s) are at the correct level if skilled individuals in the function, else would this need to be outsourced to an independent expert?	This is at the discretion of governing body/board but must satisfy the requirements of the Joint Standard.
215	ASISA	7.3(d)(iv)	The subparagraph should be rephrased to avoid an interpretation that a function or department is required for every specific risk. --- *The IT risk management framework of a financial institution must, at a minimum, encompass the following attributes and requirements –* *(d) roles and responsibilities in managing IT risks, in terms of which –* *(iv) there must be a function or department responsible for ensuring that proper risk management measures are implemented and enforced for ~~a~~ specific IT risks, and this function or department must be –*	Noted. The word 'specific' has been removed to capture collective IT risk.
216	SAIA	there must be a function or department responsible for ensuring that proper risk management measures are implemented and enforced for a specific IT risk, and this function or department must be -	It is unclear why reference has been made to "a specific IT risk" rather than IT risks as a collective within this context. It may not be feasible given the potential volume of identified IT risks and the nature, scale, and complexity of entities to establish departments per IT risks.	Noted. "Specific" has been removed from the standard to capture collective IT risk.
217	FirstRand	7.3 (d)	Governing bodies may still have overall oversight or accountability, but consideration should be given to allowing for such delegations where reference is made to specific compliance obligations (apart from the governing body's obligation to have oversight and ultimate accountability	See response to comment 212.
218	J Hayden	7.3 (d) (iii)	the governing body and senior management are fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve the performance and delivery objectives of IT investments, including their security, reliability, resiliency and recoverability.	Noted. The duty of the body is communicated earlier in the Joint Standard.
219	Clientele	7.3 d iii:	"…ensuring effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability." Achieving resiliency and recovery is certainly possible and can be well defined in terms of RTOs and RPOs. Achieving Security and reliability needs qualification in the standard, as perfect security and reliability are prohibitively expensive or even impossible to achieve and security especially has no clear industry parameters for definition.	Noted, however the standard places an obligation on the governing body to ensure that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability
220	J Hayden	7.3 (d) (iv) (bb)	headed by an individual who is part of senior management, and has the requisite qualifications (E.g., CGEIT, CRISC), knowledge, skills, and experience in IT risk management.	The Authorities are not prescriptive on this. The expectation, however, is that the function or department is headed by an individual who has the requisite qualifications.
221	Masthead	S7.3(iv)	*s7.3(iv) there must be a function or department responsible for ensuring that proper risk management measures are implemented and enforced for a specific IT risk, and this*	It is evident that only someone with the necessary skills and experience will be able to fulfil this function.

No	Commentator	Paragraph of the Standard	Comment	Responses
			function or department must be - (aa) accountable for, and be given the authority to manage IT risks; (bb) headed by an individual with requisite skills and experience, and who is part of senior management; This section indicates that the function or department mentioned in 7(iv) must be headed by an individual with "requisite skills and experience" *AND* must be part of senior management. How would smaller FSPs who do not have someone in senior management with the requisite skills and experience to manage their IT function and IT, comply with this section – in particular those that make use of third-party contractors/vendors? What would be regarded as "requisite skills and experience", and where the FSP does not have someone with such skills, would there be a transition period where someone in senior management could develop these skills and obtain relevant experience? If a transition is not possible, would the FSP have to appoint someone at senior management level to manage these risks? It is not uncommon or unreasonable for smaller financial institutions to outsource their IT support, which includes assistance in managing their IT risk. However, it appears to us, that the requirements in this section are written for large financial institutions. If our reading of this subsection is correct, then it appears that financial institutions would not be allowed to outsource their IT support since the function or department must be headed by an individual with requisite skills and experience and that person must be part of senior management. Having said this, we note that section 15 deals with outsourcing, and places a significant onus on the financial institution. We cannot agree with this onerous and prescriptive provision, and would suggest that the section should be rewritten to allow the financial institution freedom to decide its own course of action.	
222	FirstRand	7.3 (d) (iv)	The current statement can create unnecessary overhead as the requirement implies that a function or department may have to be established for each IT Risk. It must be noted that the financial institutions employ people with the requisite skills and experience for the functional and organisational role they fulfil and are given the authority to manage delivery in accordance with that. Suggest that we amend the statement to read as "*The IT risk owner remains accountable for ensuring that proper risk management measures are implemented and enforced for a specific IT risk".*	Noted. See response to comment 216.
223	BASA	7.3 (d) (iv) (aa)	BASA notes that risks can only be managed "in the work" by the technology leaders working with their counterparts in other units or functions. BASA suggests that risks cannot be managed in isolation by a separate, discrete team of people as they do not have authority for resource allocation and lack the necessary context to prioritise effectively. If this requirement is for a separate, discrete risk management function outside of IT line management such management of risks will result in a cumbersome process. BASA recommends that a better alternative may be to require specific and dedicated oversight of IT risk management.	Noted, however; the word "Specific" has been removed to capture collective IT risk.
224	BASA	7.3(d)(iv)(bb)	BASA is concerned that this may affect how members are structured. As second line IT Risk management is currently not part of senior management/"Key Persons".	Noted, however, the person must be classified as a senior manager as defined in the Joint Standard.
225	AVBOB	7.3e i and ii	What level of granularity is appropriate eg major assets like datacentre servers or even desktop computers / laptops?	This is left to the financial institution to classify.
226	FirstRand	7. 3 (e) (i) and (ii)	There exists no data structure/element in this assertion/prerequisite. While IT assets are traditionally viewed in terms of the hardware and software components, this has since evolved to consider more importantly the underlying data and its associated constructs/methods/structures and metadata. Specific mention around data and not simply "IT assets" is recommended. In addition, these statements are fairly detailed and specific, more appropriate for inclusion within an IT Asset Management Policy instead of an IT Risk Management Framework.	The Authorities have included a definition for information asset which includes data. The specificity of requirements is necessary for this standard.
227	BASA	7.3 (e)	It appears that Information Risk and Technology Risk are fluxed in this requirement. We refer to information assets under the banner of Information Risk, not Technology Risk, and this is a critical distinction as accountability for information assets vests predominantly in our members' client segments, country legal entities and client solutions,	The paragraph has been amended to cater for criticality and sensitivity of IT assets.

No	Commentator	Paragraph of the Standard	Comment	Responses
			and not in IT. Whilst identification and protection of technology assets is important, it does not appear to be the intent of this requirement, and is more than adequately addressed by broader organisational asset protection and business resilience frameworks. In keeping with contemporary governance principles technology risk and information risks should each receive specific focus. BASA suggests that consideration be given to adopting the approach of APRA CPS 234 which defines the prioritisation of IT assets in terms of (i) sensitivity - the potential impact of a loss of confidentiality or integrity; and (ii) criticality - the potential impact on the loss of availability. Consideration should be given to expanding on IT Assets to include IT Infrastructure Physical security.	
228	FEMA	7.3 (f)(ii)	Further clarity is required around the required format and minimum content of the threat and vulnerability matrix.	The Authorities are not prescriptive on the format and minimum content of the threat and vulnerability matrix, as it is performed based on nature, size and complexity of the financial institution. However, the Authorities will consider providing bilateral guidance on the matter on a case-by-case basis.
229	Telesure	7.3 (f)	Clarity is needed on the frequency of the risk assessments requirements – will an annual, comprehensive assessment suffice along with treatment plan and tracking?	Refer to paragraph 7.2 of the Joint Standard.
230	BASA	7.3 (f)	BASA notes that the requirements of this clause are generically applicable to all risk management processes and are not specific to IT risk. We suggest that these be incorporated in an over-arching risk management or enterprise risk management framework, and for this Standard to include only IT risk specific requirements to augment the over-arching Standard.	The Authorities acknowledges that the requirements of this paragraph might be applicable to other risk management processes. Paragraph 7.1 has been amended to cater for enterprise risk management.
231	BASA	7.3.(f)(ii)	BASA suggests that the identification and assessment of risk in terms of likelihood and impact, against an institutions' relevant risk matrices / appetites, should be the basis of risk mitigation and prioritisation. We note that it is not practical nor should it be mandated to additionally develop a threat / vulnerability matrix and therefore we recommend that this be removed from the standard.	The Joint Standard prescribes a threat and vulnerability assessment. Also see response to comment 228.
232	FirstRand	7.3 (f) (ii)	It is noted that the method of assessing impact could vary per institution, and still be appropriate. Impact assessment matrices could include (likelihood vs impact or frequency vs severity etc.). Additionally, we would like to work towards using the same method of assessing impact across risk types and prescribing this would prevent this within institutions. Suggest that we replace with something like "*develop a method of assessing impact of the threat to its IT environment which should also assist the financial institution in prioritising IT risks*;".	Noted, the 7.3(f)(ii) has been amended to: "develop a method of assessing impact of the threat and vulnerability to its IT environment which should also assist the financial institution in prioritising IT risks;".
233	BASA	7.3.(g)	BASA notes that the requirements of this clause are generically applicable to all risk management processes and are not specific to IT risk. We suggest that these be incorporated in an over-arching risk management or enterprise risk management, and for this Standard to include only IT risk specific requirements to augment the over-arching Standard. Specifically, BASA notes that 'Insurance' is not a form of risk mitigation but is risk transference. We also suggest that it should not be a mandatory obligation defined in a Standard and we recommend consideration should be given to its removal or rewording it to state that an institution *"may"* consider insurance as other treatment options may be more appropriate.	Noted. Paragraph 7.1 has been amended to cater for enterprise risk management. The sub-paragraph requires the financial institution to **consider** insurance as part of its risk mitigation strategy. It is not a requirement to have insurance.
234	FirstRand	7.3 (g) (iv)	Suggest removing this statement as institutions would consider all risk management actions available for treating a risk, of which insurance is one. The institution would consider those which are most appropriate for the type of risk and potential severity of impact it faces. If statement is going to remain in the standard, consider changing to *'should'* as opposed to a 'must".	Noted. The sub-paragraph requires the financial institution to **consider** insurance as part of its risk mitigation strategy.
235	FirstRand	7.3 (g) (iv)	There is no mention of external supervisory/audit functions in the practice of monitoring and managing risks. While internal components of IT and Risk management perform self-assessments etc, the element of external assurance is not only relevant but compulsory. Therefore, in relation to (iii) of the same portion of the document, engaging audit and industry expertise to define suitable remediation programmes is necessary. Assuming all the skills to mitigate and manage emerging and new risks is contained within the financial institution is not prudent.	Independent review has been defined to include internal audit as well as independent control functions.

No	Commentator	Paragraph of the Standard	Comment	Responses
236	ASISA	7.3(g)	Considering subparagraphs (i) to (iv) of subparagraph (g), it is believed that it is more appropriate to refer to the managing risks as opposed to mitigating risks. ---------- *The IT risk management framework of a financial institution must, at a minimum, encompass the following attributes and requirements –* *(g) implementation of appropriate practices and controls to ~~mitigate~~ manage risks in terms of which -*	Noted. Paragraph 7.3(g) has been amended to change mitigate to manage and 7.3(g)(ii) has accordingly been amended to remove 'manage' and replace with 'mitigate'.
237	Hollard	7.3 (h)	The line below should refer to 'major or significant' changes, as the IT ecosystem changes often with deployed changes and improved processes. "… risk assessments must include changes in systems, environmental or operating conditions that would affect risk analysis..."	Noted, the paragraph has been amended
238	AVBOB	7.3 h	Does the risk profile referred to have to be independently derived / or provided by an independent expert?	Not necessarily, however an independent expert could also provide input to the risk profile.
239	GenRe	7.3 (h) (i)	"the financial institution must maintain a risk register which facilitates the monitoring and reporting of risks. Risks of the highest severity must be accorded top priority and monitored closely with regular reporting to senior management and the governing body on the actions that have been taken to mitigate such risks. A financial institution must update the risk register periodically, and institute a monitoring and review process for continuous assessment and managing of risks and to facilitate risk reporting to management". Closely, regular, continuous – can this be defined more clearly in the standard?	Noted, the words closely and continuous have been deleted.
240	BASA	7.3 (h)(i)	BASA notes that risk registers are not an IT specific risk management requirement and it may be undesirable to have a discrete risk register for IT risks. This is because the risk response strategy for an IT risk always requires consideration of the broader risk profile and context, and often involves prioritisation and trade-offs between IT risks and other risks. BASA suggests that this can only be effective if there is a consolidated risk register addressing all risk types, with each risk tagged with risk types affected to allow for analysis and reporting by risk type. This, again, is a broader risk management requirement and we recommend that it belongs in an over-arching risk management standard rather than an IT specific one.	The Authorities acknowledges that the requirements of this paragraph might be applicable to other risk management processes; however, for the purpose of this Joint Standard, it is important that we specify these requirements. The IT risk register may be incorporated with an enterprise-wide risk register.
241	GenRe	7.3 (i) (i)	"…the financial institution must ensure careful screening and selection of staff, vendors and contractors in order to minimise IT risks due to system failure, internal sabotage or fraud" Would this be similar to Prudential Standard GOI 4 - Fitness and Propriety? If not, what screening requirements are anticipated?	There might be some commonalities between this Joint Standard and GOI 4. The financial institution must come up with its own screening and selection policies based on its requirements. Further guidance may be provided by the Authorities should be become necessary.
242	Outsurance Insurance Company	7.3(i) (ii)	We take note of the definition of fit and proper: *'fit and proper' means a person complying with any applicable fit and proper requirements imposed on such person by a financial sector law or by a financial institution who has authorised such person to access the financial institution's systems;* We understand the fit and proper requirements applicable to be the fit and proper requirements as set out in terms of the definition of fit and proper requirements in the proposed Joint Standard: '*fit and proper requirements' means requirements relating to —* *(a) honesty and integrity;* *(b) good standing;* *(c) competence, including —* *(i) experience or expertise;* *(ii) qualifications; and*	This Joint Standard does not prescribe fit and proper requirements and as such other financial sector laws applicable to the financial institution must be taken into account with regard to fit and proper requirements. In terms of vendors and contractor relating to IT, it is the duty of the financial institution to ensure per its own policies to ensure that such persons are fit and proper.

No	Commentator	Paragraph of the Standard	Comment	Responses
			technical knowledge of IT solutions and IT risks as the case may be; *If this is the intention we kindly request that the definition of fit and proper be reconsidered to provide clarity around this aspect. It is our submission that there are a number of fit and proper requirements applicable to different financial institutions and using the words 'a financial sector law' is very wide and could lead to uncertainty. We suggest the definition be amended as follow to clarify this.* *'fit and proper' means a person complying with any applicable fit and proper requirements imposed on such person* ***by this Joint Standard*** *or by a financial institution who has authorised such person to access the financial institution's systems*	
243	Telesure	7.3 (i) (ii)	Fit and Proper – to what level will the fit and proper assessment need to go? Will the expectation be to maintain a fit & proper register?	This Joint Standard does not prescribe fit and proper requirements and as such other financial sector laws applicable to the financial institution must be taken into account. Refer to the response to comment 242 above.
244	Maitland	7.3 (i)(ii)	All staff have access to the financial institutions' systems in line with the staff member's job requirements. The normal employment screening process combined with the confidentiality requirement in the staff member's contract of employment and the security safeguards implemented by the financial institution are reasonable measures to protect sensitive or confidential information. Vendors are subject to due diligence processes and required to complete non-disclosure agreements. The level of competence in terms of technical knowledge of IT solutions and IT risks will vary significantly depending on whether the staff member is junior member of staff or a senior IT manager. Is it the intention to conduct a fit and proper test for every staff member and vendor? We submit that conducting fit and proper tests on all staff and vendors is an onerous provision.	This must be read with the definition of "fit and proper".
245	FirstRand	7.3 (i) (iii)	The training requirement statement is very broad and can be interpreted widely. In its widest sense, it can be interpreted to be that all staff, contractors and vendors who have access to IT resources, infrastructure and systems must undergo every training program in the group. In reality, not all staff/contractors/vendors are required to do the same training as these are mostly role dependent. FirstRand therefore recommends that the second sentence be amended to "*T*he relevant training programmes must be extended to all eligible new and existing staff, c*ontractors and vendors who have access to the financial institution IT resources, infrastructure and systems".* FirstRand also notes that IT resource/s has not been defined and may further widen the interpretations of the above section.	Noted. The standard has been amended to include 'relevant' and delete 'resources'. It will now relate to IT infrastructure and systems.
246	Hollard	7.3 (i) (III)	The statement below is too widespread. Relevant training programmes are role and access based for IT staff and contractors who have access to systems. "The training programmes must be extended to all new and existing staff, contractors and vendors who have access to the financial institution IT resources, infrastructure and systems;"	Noted. The standard has been amended to include 'relevant' and delete 'resources'. It will now relate to IT infrastructure and systems.
247	Brightrock	7.3(I)(iii)	Please provide clarity on "training programmes" – what training are you referring to?	The training programmes will relate to IT risk. The Joint Standard has been amended to include the word 'relevant' before training.
248	Maitland	7.3 (i)(iii)	Vendors and contractors are selected for their expertise and are subject to non-disclosure agreements. It should not be the responsibility of the financial institution to train vendors and contractors.	It is the duty of the financial institution to limit IT risks. Consequently, it must ensure that the staff, contractors and vendors who have access to the institution's IT resources, infrastructure and systems, receive training to limit those risks.
249	BASA	7.3.(i)(iii)	BASA suggests the following wording: "organisations/institutions will determine which training programs are required, to whom it will be applicable including frequency of retraining. Required training programmes, including training materials, must be acquired, or developed and endorsed by senior management, be reviewed ahead of each new campaign. The training programmes must be extended, where applicable, to all new and existing staff, contractors and vendors who have access to the financial institution IT resources, infrastructure and systems.	Noted, the Authorities disagree. The wording provided under the paragraph is sufficient to provide a requirement to develop its training programmes and materials.

No	Commentator	Paragraph of the Standard	Comment	Responses
250	AVBOB	7.3 i (iii)	Are senior management the correct level of resource to endorse training materials?	The Authorities are of the view that, given the importance of this training, senior management must endorse the training materials.
251	Masthead	S7.3(i)	*s7.3 (i) people management in terms of which –* *(i) the financial institution must ensure careful screening and selection of staff, vendors and contractors in order to minimise IT risks due to system failure, internal sabotage or fraud;* *(ii) staff, vendors and contractors, who are authorised to access the financial institution's systems, must be fit and proper and be contractually required to protect sensitive or confidential information;* *(iii) training programmes, including training materials, must be acquired or developed and endorsed by senior management, and be conducted and reviewed regularly, but at least annually. The training programmes must be extended to all new and existing staff, contractors and vendors who have access to the financial institution IT resources, infrastructure and systems; and* *(iv) such updates, made as a result of the review conducted in terms of item (iii) above, must ensure that the contents of the training programme and material remain current and relevant. Such updates must also take into consideration the evolving nature of technology as well as emerging risks.* We note that the fit and proper requirements apply to all contractors and vendors who must be fit and proper, which includes aspects such as qualification and experience. We wonder how these requirements would apply to contractors, vendors and staff who are not also authorised financial services providers (representatives or key individuals), e.g. data storage facility/provider's staff? In our view, it is not reasonable to expect that the full gamut of fit and proper requirements should extend to these persons. If, despite our reservations, it is the intention tp apply all these fit and proper requirements, it seems that an FSP would need some level of due diligence or declaration process for vendors and contractors who access the FSP's systems? This raises various questions, like (1) who does the screening/due diligence, (2) what level of screening is required, (3) is a due diligence done at organisational level or at individual level, (4) what level of responsibility does the FSP have in terms of ongoing checks? We question the desired outcome or course of action should an existing contractor or vendor be found not to be fit and proper? Due to the nature of the type of relationship and services, an abrupt termination or change of provider could place the FSP and its clients at risk, which in our view is not the intended outcome of this regulation. We request further guidance on the application of these fit and proper requirements, as well as detail on remedial actions in the event of non-compliance.	The requirement to be fit and proper applies only to staff, vendors and contractors who are authorised to access the financial institution's systems, and only insofar as fit and proper requirements are imposed by a sectoral law. Should a staff member, vendor or contractor not be fit and proper, the financial institution should not allow that person access to its systems. In addition, that person would be in contravention of the requirement of the relevant sectoral law, and the institution would have to follow the necessary steps for dealing with non-compliant persons as provided for in that sectoral law.
252	J Hayden	7.3 (j)	An IT control framework such as COBIT as a reference for the design and implementation of the IT control environment.	The Authorities do not prescribe a preferred framework as this choice must be made by the relevant financial institution. The Authorities however, expect that the requirements of this Joint Standard are met when applying a particular framework.
253	PSG Konsult		No comment	Noted
254	SAIS		No comment.	Noted
255	Ubank		No comment	Noted
256	Assupol Group		No comment.	Noted
257	Maynard Bester (ISACA member)		No comment.	Noted
258	BDO		No comment	Noted
259	GENERIC Insurance Company		No comment	Noted
260	SAHL		No comment	Noted

No	Commentator	Paragraph of the Standard	Comment	Responses
261	BNP Paribus		No comment	Noted
8. Oversight of IT risk management				
262	SAIA	Oversight of IT risk management must be incorporated into the governance and risk management structures, processes, and procedures of a financial institution, including provisions relating to direct reporting lines to the governing body.	a) In consideration of a group structure with multiple licensed financial institutions, is it the Authorities' intention to require the oversight of IT risk management at the group governing body level or at a financial institution/ financial service provider governing body level? b) One member submits that for some groups, which may include listed companies, each subsidiary, and the controlling company adhere to the principles and recommendations of the King IV Report on Corporate Governance, notwithstanding that it is not legislated. It is therefore recommended that the requirements of the Joint Standard be aligned to the King IV Report.	The Authorities are of the view that if the financial institution is licensed for more than one activity, each entity licensed must comply based on the size nature and complexity irrespective of where controls have been defined from. The minimum requirements are the same for the various financial institutions and the financial institution must apply the principles based on the nature, scale and complexity. With regard to bank controlling companies and insurance group, the requirements apply at a consolidated level and a solo level. Each financial institution captured by this Joint Standard must be able to prove compliance with the requirements on institution-specific risk whether it is captured at an institution level or at a group level. The Authorities do not prescribe a particular governance code/framework as this choice must be made by the relevant financial institution. The financial institution must ensure that it complies with the provisions of this Joint Standard.
263	FirstRand	8	Regulation needs to be balanced between principles and rules. We suggest that the reporting line structure is informed by the organisational roles and responsibilities as specified by mandated senior executives outside of the governing body. With regard to the reference to "direct reporting lines to the governing body": we suggest that the reporting line structure should be informed by the organisational roles and responsibilities as specified by mandated senior executives, who may potentially have reporting lines outside of the governing body.	Noted. The paragraph has been amended to remove the word "direct"
264	Masthead	S8	*s8 - Oversight of IT risk management must be incorporated into the governance and risk management structures, processes and procedures of a financial institution, <u>including provisions relating to direct reporting lines to the governing body</u>.* The fact that there is an expectation that there is a direct reporting line to the governing body seems to imply that such oversight cannot be done by an external party? If this is the intent, then we find it very restrictive and we cannot agree with this provision. We would suggest that the underlined wording above be deleted.	Disagree. A financial institution is allowed to outsource its IT (in accordance with the Standard) but, even then, it is still the responsibility of the institution to comply with the requirements and the governing body should therefore ultimately have oversight of IT risk management.
265	BASA	8	Must this oversight of IT be independent of IT first line? i.e. a second line function like risk management or compliance or must it be an independent expert?	It must be an independent function such as second line. It is not requirement that you have an independent expert.
266	BASA	8	BASA suggests that more explicit requirements should be included in the Standard for it to be meaningful, and to set out specific expectations for oversight activities, roles, and / or structures. BASA also seeks clarity on whether this only refers to Board/Governing body oversight or also to the oversight of the Second Line of Defence (SLOD) over a First Line of Defence (FLOD) IT Risk function? The reporting line structure should be informed by the organisational roles and responsibilities as specified by mandated senior executives, who may potentially have reporting lines outside of the governing body.	It must be an independent function such as second line. The governing body is ultimately responsible for oversight. Please refer to the requirement of paragraph 5.3. Also see response to comment 263.
267	SAIS		No comment	Noted
268	PSG Konsult		No comment	Noted
269	Assupol Group		No comment	Noted
270	Maynard Bester (ISACA member)		No comment.	Noted

No	Commentator	Paragraph of the Standard	Comment	Responses
271	BDO		No comment	Noted
272	HBZ		No comment	Noted
273	FEMA		No comment	Noted
274	ASISA		No comment	Noted
275	ECIC		No comment	Noted
276	GENERIC Insurance Company		No comment	Noted
277	JSE		No comment	Noted
278	Ubank		No comment	Noted
279	J Hayden		No comment	Noted
280	Maitland		No comment	Noted
281	SAHL		No comment	Noted
282	GenRe		No comment	Noted
		9. IT operations		
292	AVBOB	9.1	No mention of board approved or endorsed? However, 9.3 (a) seems to imply this as it states that "A Financial Institution must" which implies that the governing body as this responsibility. Seems very operational - Managing ICT process and procedures. What level of policies are the governing body expected to approve?	Noted, paragraph 9.3 has been amended to remove the requirement for board approval.
293	FirstRand	9.1	It is noted here that an institution may have various processes and procedures and policies covering IT Service Management domains, which together make up a "Framework". The expectation here should not be that institutions create a singular "Framework" document. Hence suggest amending the wording to "*A financial institution should develop a robust set of IT Service management policies, standards, procedures and processes which is essential……..production IT environment*.".	Noted. Paragraph 9.1 of the Joint Standard has been amended accordingly.
294	BASA	9.1	BASA would appreciate clarity on the aspect of IT Service Management Framework and whether this be any other Technology or related management framework/Policy.	Noted. Paragraph 9.1 has been amended to the suggested wording.
295	FirstRand	9.2	Following on from the previous comment, suggest that this statement be reworded to "*IT Service Management must comprise a governance……capacity management*.".	Noted. Paragraph 9.2 has been amended.
296	JSE	9.2	Clarity is sought on whether 'capacity management' refers to human capacity, technology capacity, or both.	In the context, the term refers to both human and technology capacity.
297	Masthead	S9.3	*TYPO: s9.3(a) "… and must enable financial institution …"* should read *"..must enable **the** financial institution …"*	
298	JSE	9.3(a)	The sub-paragraph provides '…manage its IT operations based on documented and implemented policies, processes and procedures that are approved by the governing body'. While we agree that the governing body should approve policies, it is our view that it would inappropriate, impractical and costly for a governing body to approve IT operations' processes and procedures.	Noted, see response to comment 292.
299	FirstRand	9.3 (a)	a) Documenting of critical IT operations – can this be reworded to maintaining a register of critical IT applications?	Noted, paragraph 9.3 (a) has been amended accordingly.
300	ASISA	9.3(a)	It is not current practice for governing bodies to approve operational policies, processes, and procedures. As is required by the Draft Joint Standard, a governing body approves the IT strategy and IT risk management framework. Senior management is then responsible for the operational policies, processes, and	Refer to the response to comment 292.

No	Commentator	Paragraph of the Standard	Comment	Responses
			procedures that would support the IT strategy and IT risk management framework. Governing bodies generally delegate operational implementation to senior management. Paragraph 9.3(a) should be amended accordingly. ---------- *A financial institution must -* *(a) manage its IT operations based on documented and implemented policies, processes and procedures ~~that are approved by the governing body~~*.	
301	Hollard	9.3 (a)	Can the governing body delegate the approval of some of the policies, processes, and procedures to the relevant stakeholders in the business?	Refer to the response to comment 292.
302	BASA	9.3(a)	BASA is concerned that there may be potential for the requirement that the Governing Body must approve a whole suite of IT operational policies, procedures and process documents may become too onerous on the Board/Governing Body. We suggest that it may make more sense for the Board/ Governing Body to approve relevant policies, for senior management" / Key Person/s to approve procedures and process documents. We also suggest that consideration should also be given to the fact that there are multiple governing bodies including board and executive level ones, and we recommend that more practical wording may be manage its IT operations based on documented and implemented policies, processes and procedures that are approved by **appropriate governing bodies** ~~the governing body~~.	Refer to the response to comment 292.
303	Clientele	9.3.b.	"…maintain and improve efficiency…" are very desirable and indeed every organisation should aspire to these, but I believe it is not sufficiently definable to include in a standard. During system transitions and significant changes efficiency can worsen for a short period at an acceptable cost, versus the prohibitive cost of guaranteeing that efficiency always improves. The second part of 9.3.b I agree with and the paragraph could start at "minimise potential incidents…" To require that an organisation should have a continuous improvement process is also fair.	Noted, the paragraph has been amended to remove the word 'improve.
304	BASA	9.3 (c)	BASA suggests that there are widely divergent views as to what constitutes "critical" IT operations and a definition would be beneficial.	Noted, the paragraph has been amended.
305	Clientele	9.3.d.	Define a "proper configuration management process". Aeroplane manufacturers do this well at great cost, because lives could be lost if they do not. Many banks have attempted to do this well and failed at great cost. Configuration management should be appropriate to the importance and complexity of the systems and can often be designed to be self-documenting. Achieving configuration management using a single unified configuration management system (requiring integration to the infrastructure and software configuration management tools) versus using separate fit-for-purpose systems for Infrastructure, and Software have fundamentally different overheads, complexities and costs, but can be equally effective. Thus, I request a better definition for "proper".	Noted, the paragraph has been amended.
306	Hollard	9.3 (d)	Is this mainly for core IT assets?	No, it is for all IT assets
307	BASA	9.3 (f)	If the Standard addresses information risk as well as technology risk (BASA recommends throughout our comments, that they should be separated), then this requirement should be extended to retention periods for information and data. It is also noted that King differentiates this.	Noted and the paragraph has been amended to remove the word 'data'
308	FirstRand	9.3 (f)	FirstRand recommends that any statement in the standard which makes reference to information or data be removed from this standard as this is broader than just IT. It is also noted that King IV now specifically differentiates this.	Noted and the paragraph has been amended to remove the word 'data'
309	BASA	9.3 (g)	BASA recommends that the term "change control" be used in this context instead of 'change management process' to distinguish from organisational and people change management.	The paragraph has been amended to include the word 'IT' before the 'change management'
310	FirstRand	9.3 (g) + 9.3 (h)	There are elements of duplication here and in 9.2 e.g. requirement for incident and change process.	Noted, paragraph 9.2 has been amended.
311	ASISA	9.5	The reference to "testing" causes confusion because testing could be integrated in stages of development and be dealt with differently depending on the development process. It is proposed that paragraph 9.5 should be rephrased to require appropriate segregation of duties between development and production environments. ---------- Noted, the paragraph has been amended.	Noted. Paragraph 9.5 has been amended to read: "A financial institution must implement appropriate segregation of duties between the development, testing and operations functions environments".

No	Commentator	Paragraph of the Standard	Comment	Responses
			A financial institution must ~~enforce~~ ensure appropriate segregation of duties ~~for the~~ between development~~, testing and operations functions~~ and production environments.	
312	FirstRand	9.5	This assertion is contentious and results in audit findings in many financial institutions in that while environments should be logically separate in textbook situations, in practice this is often not the case due to cost, resources and various other factors, for example, the practice in IT Operations has migrated to Agile methods where resources perform development and operation functions, or even development, security and operational functions, or known as “DevOps” and “SecDevOps”. Therefore, this waterfall methodology will be almost unenforceable going forward. We would therefore require a stipulation that adequate controls are implement environmentally and where user access is concerned to ensure adequate logging, monitoring and reporting where the combination of roles is not only possible, but also required to achieve agile outcomes. Certain controls, however, can be enforced through the development life cycle standards. We could reword here to state something like “*Developers should not have the ability to deploy their own code into production*.” Other suggestion would be to include establishment of compensating controls where strict enforcement is not viable as follows: “*A financial institution must enforce segregation of duties for the development, testing and operations functions. Where full enforcement of segregation of duties cannot be achieved, compensating controls must be established to provide control over activities not commensurate with function roles and the risks involved*”	Noted, however this is dependent on differing environment with the financial sector, not every institution is following the same methodology. If compensating controls were to be implemented, internal governance process should be followed. Paragraph 9.5 has been amended to read: A financial institution must implement appropriate segregation of duties between the development, testing and operations functions environments.
313	JSE	9.5	The segregation of the development, testing and operations functions is a control feature of a traditional waterfall approach to a technology project or programme. Many financial institutions have adopted an Agile methodology which provides a DevOps approach which, *inter alia*, combines software development and IT operations. Agile methodology is an internationally accepted and widely adopted methodology. A DevOps approach is implemented to iteratively deliver high-quality software at a faster pace than the traditional waterfall approach. We respectfully request that the Authorities consider the impact of paragraph 9.5 on the ability of financial institutions to comply with this requirement without having to revert to a waterfall approach at great expense.	See response to comment 311 above.
314	Maitland	9.5	We suggest that the wording be amended as follows: A financial institution must enforce segregation of duties *where feasible, based on the nature and size of the financial institution,* for the development, testing and operations functions.	Noted. Paragraph 9.5 has been amended to read: A financial institution must implement appropriate segregation of duties between the development, testing and operations functions environments.
315	Masthead	S9.5	s9.5 *A financial institution must enforce segregation of duties for the development, testing and operations functions* In the context of smaller financial institutions (discretionary FSPs), this requirement may not be practical. In such a case, between section 4.3 and this section, which one prevails?	See response to comment 314.
316	BASA	9.5	BASA suggests that this needs to be expanded to define the expectation for segregation of duties. Specifically, whether this refers to a segregation regarding roles and / or segregation regarding environments (development / test / production). On a practical level in institutions, while environments should be logically separate in textbook situations, in practice this is often not the case due to cost, resources and various other factors, for example, the practice in IT Operations has migrated to Agile methods where resources perform development and operation functions, or even development, security and operational functions, or known as “DevOps” and “SecDevOps”. Therefore, this waterfall methodology will be almost unenforceable going forward. We would therefore suggest that a stipulation that adequate controls are implemented environmentally and where user access is concerned to ensure adequate logging, monitoring and reporting where the combination of roles is not only possible, but also required to achieve agile outcomes. Certain controls, however, can be enforced through the development life cycle standards.	Noted, however this is dependent on differing environment with the financial sector, not every institution is following the same methodology. If compensating controls were to be implemented, internal governance process should be followed. Paragraph 9.5 has been amended to read: A financial institution must implement appropriate segregation of duties between the development, testing and operations functions environments.
317	AVBOB	9.5	Could this statement please be clarified. What does it mean and who will enforce this segregation?	Noted, the paragraph has been amended.

No	Commentator	Paragraph of the Standard	Comment	Responses
318	Clientele	9.5.	Dev-ops is a commonly used approach and insisting on segregation of duties is dated. Rather, for example, the risk of code being deployed that has not first passed through the Testing and User Acceptance phases should be prevented. If the same developer then deploys code using this approach, there is no additional risk. Modern source control and deployment systems control the flow of code through the Development, Test, User-Acceptance, Pre-production and finally Production environments such that tampering is not possible without restarting the process from the beginning each time code is modified. Although it is possible to achieve segregation of duties using the same tools, it is much more costly from a resourcing perspective, with little risk reduction.	Noted, however this is dependent on differing environment with the financial sector, not every institution is following the same methodology. If compensating controls were to be implemented, internal governance process should be followed.
319	SAIA		No comments.	Noted
320	SAIS		No comments.	Noted
321	PSG Konsult		No comments.	Noted
322	Assupol Group		No comments.	Noted
323	Maynard Bester (ISACA member)		No comment.	Noted
324	BDO		No comment	Noted
325	HBZ		No comment	Noted
326	FEMA		No comment	Noted
327	ECIC		No comment	Noted
328	GENERIC Insurance Company		No comment	Noted
329	Ubank		No comment	Noted
330	J Hayden		No comment	Noted
331	SAHL		No comment	Noted
332	GenRe		No comment	Noted
333	BNP Paribus		No comment	Noted
10. Information security				
334	BASA	10	BASA notes that information security is a discrete discipline, separate from IT risk, and is already largely addressed in cyber security and cyber risk regulations and laws. We suggest that if there is a need for additional standards in this regard over and above the already issued cyber resilience guidance notes, laws, regulations or standards, that these should be issued separately from an IT risk standard. Another view is that whist it is a distinct discipline, IT Security Risk and Cybersecurity Risk management still forms part of the banks' IT Risk functions and their staff resources will refer to this (IT Risk Management) standard for guidance. Therefore, the suggestion is that only a few key high-level principles be included in this document, with references to the already existing cyber security and cyber risk regulations and laws	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
335	BASA	10.1	Please refer to our general comments below at (4) specifically.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.

No	Commentator	Paragraph of the Standard	Comment	Responses
336	Hollard	10.1	Recommend reword statement to add the word 'known' between the words 'all and forms' in this section: "…all forms of security vulnerabilities."	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
337	BASA	10.2	BASA suggests that consideration should be given to merging Clauses 10 and 12 as both are related to Information Security, with a flavour of Cyber/Cyber related to product.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
338	ASISA	10.2	Paragraph 10.2 of the Draft Joint Standard should be simplified to avoid uncertainty in relation to technical terms. --- *A financial institution must establish ~~measures that protect at-rest, in-transit and in-storage,~~ data protection measures commensurate with the criticality of the information held, also extending to backup systems and offline data stores.*	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
339	BASA	10.3	In this information security section (or section 9 relating to IT operations), BASA suggests that a requirement should be added related to legacy systems that are no longer supported and for which security updates are no longer developed. We recommend that plans should be put in place to manage risks associated with these systems and the vulnerabilities that an institution may be exposed to.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
340	ASISA	10.3(a)	The reference to "expected level of protection" may cause uncertainty as to who creates the expectation of the level of protection. It is therefore suggested that the reference to "expected" be replaced with a reference to "appropriate", --- *A financial institution must –* *(a) configure IT systems and devices with security settings that are consistent with the ~~expected~~ appropriate level of protection.*	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
341	FirstRand	10.3 (a)	FirstRand recommends that the wording be changed from "Baseline standards must be established for key technologies", to Baseline standards are not defined for all applications, but rather underlying key technologies e.g. operating systems, database etc. FirstRand suggest that the wording should be changed to read: to "*Baseline standards must be established for key technologies"*	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
342	AVBOB	10.3 (a)	The requirements seem very granular for regulatory purposes and might be prohibitive for smaller players with outsourced systems. Limited reference to cloud applications and computing? Are baseline standards defined? Baseline standards that are acceptable to who – governing body, external auditors etc?	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
343	BASA	10.3 (a)	BASA notes that this provision determines that a financial institution must establish baseline standards to facilitate consistent application of security configurations for operating systems, applications, databases, network devices and enterprise mobile devices within the IT environment. In other paragraphs (for example 12.2) reference is made to adhering to "well-established and adopted international standards". BASA seeks clarity on whether the institution can determine whether the baseline standards are reasonable, or whether the intent of the Authority is to measure baseline standards against established and adopted international standards. In addition, we suggest the following wording: "*Baseline standards must be established* **for key technologies** ~~to facilitate consistent application of security configurations for operating systems, applications, databases, network devices and enterprise mobile devices within the IT environment~~;	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
344	Brightrock	10.3(a)	Are baseline standards expected to be defined as a whole for the industry, or will these be set by each financial institution given each's maturity and IT risk profile?	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
345	BASA	10.3(b)	BASA recommends that the word "enforcement" in both sentences be replaced with the word "compliance". BASA suggests that information be provided on who is responsible to conduct these reviews (i.e., FLOD security teams or SLOD risk teams, e.g., IT Risk teams within an Ops Risk or ERM function)	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.

No	Commentator	Paragraph of the Standard	Comment	Responses
346	Masthead	S10.3(b)	*TYPO: s10.3(b) – in this subsection there is reference to "item (a)". We suggest that this should read "subsection (a)".*	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
347	Assupol Group	10.3(e)	We recommend the addition of the concept of "end point security" as part of paragraph 10.3(e) as opposed to "Antivirus software" which only looks at possible virus attacks yet there are numerous attacks that have been acknowledged that fall under the terminology "end point" to encompass all.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
348	BASA	10.3.e	BASA notes that this applies to traditional antivirus (AV) vendors, but not Next Generation Anti-Virus (NGAV) solutions. Many companies now use advanced anti malware such as Endpoint Detection and Response (EDR) and Software as a Service (SaaS) -based solutions that do not work on the traditional AV model. Regular scans are not required as the technology is always monitoring and analysing the device. The wording needs to be updated to accommodate these technologies. Also, AV is being very prescriptive and perhaps too specific, and therefore BASA recommends that reference rather be made to 'Malware protection'. This allows institutions to decide on the correct approach for their environment.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
349	BASA	10.3(f)	BASA suggests the following wording: "*regularly review security logs of* **key** *systems, applications and network devices for anomalies following a risk-based approach*;	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
350	FirstRand	10.3 (f)	FirstRand suggest a wording change to "regularly review security logs of key systems, applications and network devices for anomalies following a risk-based approach"? The Bank performs threat modelling and focusses on streaming logs and alerts from key systems to monitor security risk as a risk-based approach.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
351	BASA	10.3.g	BASA recommends the inclusion of a frequency, or at wording to the effect of "in line with internal assessments / internal processes". We note that this paragraph details that "reviews of the information security framework must be subject to independent audit assessments, and the results of the review must be reported to the governing body. Clause 16(2)(a) specifically refers to the internal audit function of a financial institution. BASA seeks clarity on whether this refers to the internal audit assessment and if so, we suggest an amendment to the paragraph to expressly refer to the fact that the impendent audit assessments be carried out by the internal audit function.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
352	Masthead	S10.3(g)	s10.3(g) requires that reviews of the information security framework must be subject to independent audit assessments. Similar to our earlier responses/comments, our view is that to prescribe independent audit assessments is onerous and potentially costly for smaller financial institutions. We would therefore suggest that this is not made an absolute requirement.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
353	ASISA	10.3(g)	It is presumed that the required independent audit assessment may be performed by an internal audit/control function as referred to in paragraph 16.1 of the Draft Joint Standard. The cost of an external assessment independent of the financial institution would be unreasonable. Paragraph 10.3(g) should be amended for the sake of clarity and to improve reading thereof. --- *A financial institution must –* *(g) ensure that reviews of the information security framework ~~must be~~ are subject to independent audit assessments by an internal control function as referred to in paragraph 16.1 of this Standard, and the results of the review must be reported to the governing body.*	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
354	Maitland	10.3 (g)	We suggest that the wording be amended as follows: reviews of the information security framework must be subject to independent *internal* audit assessments, and the results of the review must be reported to the governing body	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
355	BNP Paribus	10.3 (g)	10.3 (g) - Could the Information Security Framework Assessment be performed by Internal Audit or by External Auditor and at what frequency?	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.

No	Commentator	Paragraph of the Standard	Comment	Responses
356		10.3(g)	"Reviews of the information security framework must be subject to independent audit assessments, and the results of the review must be reported to the governing body" What is considered as independent reviews? Could this involve the Internal Audit of the company? How regular would these assessments be required?	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
357	Maynard Bester (ISACA member)	10.3 (h)	regular penetration testing of the "crown jewels" to ascertain whether the security controls are preventing external threat actors from gaining unauthorised access as well as gauging whether the simulated attack/hack is detected (as referenced in paragraph 10.3 (f))	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
358	JSE	10.3(2)	See general comment below in respect of the use of the term 'enterprise'.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
359	FirstRand	General	FIs may share information with the Regulators from time to time, as required under existing financial sector laws. Will the IT teams from the Authorities be initiating conversations and collaborating with FIs/industry bodies to find more secure ways of sharing information – to assist with compliance with this Standard?	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
360	FirstRand	Overall	Section 10 of the proposed standard outlines requirements for "Information security". - Its opportune time to introduce the Cybersecurity / Cybersecurity Risk as a sub-domain of this standard. - This is a growing area of concern given that: - most financial institutions are driving more and more digital strategies, - there is growth seen in cyber threats and related attacks, - prevailing developments in the country legislations (e.g. introduction of the Cyber Crimes Act in SA) - the ongoing demands by other industry bodies for transparency in adopted cyber security approaches - Disparate approaches adopted in the industry yet common risks. Etc. - This standard should make differentiation between Information Security and Cybersecurity. - Both the terms, cybersecurity and information security are associated with the security of computer systems, they both have some overlapping risk & control strategies and are often used as synonyms. However, the definition and understanding of the terms do vary and should not be interchangeable as it is done often. See example differentiation: • Cybersecurity: - - defending of computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Such attacks can be divided into categories, such as cybercrime (targeting financial gain), cyber-attacks (mostly political attacks) and cyberterrorism and these require fitting response / control strategies. • Information Security: - - Can be simply described as prevention of unauthorised access, disclosure, or alteration during the time of capturing, storing data or transferring it from one machine to another. It is created to cover three objectives of confidentiality, integrity and availability or as commonly known as CIA.	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.
361	GenRe		There are areas where the Joint Standard is much more detailed regarding the implementation of controls than the regulatory stipulations of other countries. For instance, the German (BaFin) standard describes requirements for control objectives and then allows the financial institution to decide on how to implement these controls. By comparison, in some areas, the Joint Standard requires the implementation of specific controls. For example: "implement appropriate, state of the art operational information security measures" (BaFin VAIT) vs. "deploy anti-virus software to servers and workstations" (Joint Standard 10.3 e). The requirements being highly prescriptive limits the option set for the financial institutions and may lead to the implementation and	Noted, however the paragraph has been removed from the standard as there is a separate joint standard that will be addressing these requirements.

No	Commentator	Paragraph of the Standard	Comment	Responses
			persistence of suboptimal controls as technology advances and the threat landscape changes.	
362	HBZ	All	Noted	Noted
363	SAIA		No comments.	Noted
364	SAIS		No comments.	Noted
365	PSG Konsult		No comments.	Noted
366	BDO		No comment	Noted
367	FEMA		No comment	Noted
368	ECIC		No comment	Noted
369	GENERIC Insurance Company		No comment	Noted
370	Ubank		No comment	Noted
371	J Hayden		No comment	Noted
372	SAHL		No comment	Noted
11. Sensitive and confidential information				
373	BASA	11	BASA suggests that the heading be amended to: **Protection of** Sensitive or confidential information. "sensitive or confidential information" definition must be aligned with the definitions of Personal Information and Special Personal Information in POPIA. It is also important that the use of the word "confidential" is defined if used here, as it's applicable is wider than "privacy". A reading of the draft clause 11.2 (e) suggests that the words 'sensitive or confidential information" is being used synonymously the POPIA definitions. Suggestion that this be aligned across this Standard and POPIA. BASA notes that information risk is a separate risk type and not part of IT or technology risk. This is a critical distinction as the objectives, accountability, resourcing and governance of information risk is entirely separate from IT/technology risk. BASA suggests that consideration be given to removing this from the IT/technology risk standard and addressing it separately, as supported in the King Code IV.	Noted. The heading has been changed 'Handling of sensitive and confidential information'. This section applies over and above personal information. Noted. Sub-paragraph (d) has been reworded to remove reference to privacy., i.e. A financial institution must conduct independent reviews, annually, to assess compliance with the measures implemented in terms of sub-paragraphs above. That is so far as the information is covered by the POPI Act, the POPI Act definitions will apply. The standard is specific to information stored on IT systems.
374	BASA	11.1	Given the expectation to protect data in line with its classification, BASA suggests consideration be given to including a requirement to classify data in accordance with an approved classification scheme.	Noted, the Authorities are of the view that the classification of data falls within the jurisdiction of the Information Authority.
375	BASA	11.1(a)	It is recommended that the Authority align the provisions of this clause to the definitions of POPI, as the potential to cross reference to prohibited trading practices under the Financial Markets Act, as per previous inference under clause 4.4.to consult financial sector regulation in the application of this standard, may be raised.	In so far as information is covered by the POPI Act, the POPI Act definitions will apply.
376	FirstRand	11.1 (a)	FirstRand suggest that this statement be amended to "*protect such as customer personal account and personal information, including but not limited to the POPIA designated fields and transaction data in systems*;" "sensitive or confidential information" definition must be aligned with the definitions of Personal Information and Special Personal Information in POPIA. It is also important that the use of the word "confidential" is defined if used here, as it's applicable is wider than "privacy".	This section applies over and above personal information. See responses to comments 233 and 235.

No	Commentator	Paragraph of the Standard	Comment	Responses
			A reading of the draft clause 11.2 (e) suggests that the words 'sensitive or confidential information" is being used synonymously with the POPIA definitions. Suggestion that this be aligned across this Standard and POPIA. FirstRand notes that information risk is a separate risk type and not part of IT or technology risk. This is a critical distinction as the objectives, accountability, resourcing and governance of information risk is entirely separate from IT/technology risk. FirstRand suggests that consideration be given to removing this from the IT/technology risk standard and addressing it separately. This point is reflected within King IV as well.	
377	AVBOB	11.1 (a) and 11.2 (c)	This section is already covered in terms of the POPIA Act. Is the intention of the standard to cover anything in addition?	Noted. This Standard must be read in conjunction with other applicable legislations. When the Authorities assess compliance with this Standard specific attention will be given to what is covered in this Standard
378	BASA	11.2.(a)	BASA suggests that clarity be provided regarding access as this section relates to data. We recommend amendment to the first sentence as follows: (a) define, document and implement procedures for logical access control (identity and access management). These procedures must be implemented, enforced, monitored and periodically reviewed. The procedures must also include controls for monitoring anomalies, **define, document and implement procedures for logical access control to sensitive or confidential information (identity and access management);**	Noted; however, this section does not only relate to data but to information that is stored and processed in systems. The intention is not to limit the application of this procedure to sensitive and confidential information.
379	BASA	11.2(c)	BASA requests that clarity be provided on why only information transmitted to customers is included and we suggest that information transmitted to other third parties involved in the customer value stream, e.g., business partners, such as benefits partners, should also be included	Noted, the paragraph has been amended.
380	ASISA	11.2(d)	It is presumed that the required independent reviews may be performed by an internal audit/control function as referred to in paragraph 16.1 of the Draft Joint Standard. The cost of an external assessment independent of the financial institution would be unreasonable. Paragraph 11.2(d) should be amended accordingly and the reference to "privacy policies" should be amended to "IT privacy policies" for the sake of clarity. --- *A financial institution must -* *(d) conduct independent reviews by an internal control function as referred to in paragraph 16.1 of this Standard, annually, to assess compliance with its IT privacy policies.*	Noted, the Authorities have defined 'independent review'.
381	FirstRand	11.2 (d)	"conduct independent reviews" – does internal audit satisfy this requirement from an independent perspective? This obligation is already addressed through section 19 of POPIA and the proposed additional requirement to have annual independent reviews imposed by this standard is extremely onerous and costly. Compliance with privacy policies in financial institutions will already be managed through its other risk and compliance frameworks.	See response to comment 252.
382	Brightrock	11.2(d)	Please provide clarity on "independent reviews", and what assurance providers would meet this requirement. For example, Internal Audit, Compliance, etc? Is the result of the independent reviews to be reported to the Authorities? If so, please provide clarity on the form and manner of the reporting.	See response to comment 252.
383	AVBOB	11.2 (d)	Can internal audit do this or must it be an independent (of the organisation) expert?	See response to comment 252.
384	GenRe	11.2 (d)	What is considered as independent reviews? Could this involve the Internal Audit of the company?	See response to comment 252.
385	BASA	11.2(d)	BASA suggests that the requirement to do this annually should be reconsidered as it may not be reasonable. BASA recommends to following amendments: *"A financial institution must -* *11.2(d) ~~conduct independent reviews, annually, to~~ assess compliance with its privacy policies on a regular basis. In addition, independent reviews may be used to identify*	See response to comment 252. The timeframe has been removed.

No	Commentator	Paragraph of the Standard	Comment	Responses
			vulnerabilities in compliance processes that can undermine confidential and sensitive information on its systems."	
386	Maitland	11.2(d)	We submit that the requirement for a financial institution to conduct independent reviews annually to assess compliance with its privacy policies is a wider obligation in terms of the Protection of Personal Information Act, which requirement is overseen as part of the activities by the compliance and internal audit functions as part of the 3 lines of defence model. This requirement does not appear appropriate as part of an IT Risk management framework. However we agree that the use of independent reviews to identify vulnerabilities in the compliance processes that can undermine confidential and sensitive information on its systems is appropriate as part of an IT risk management framework.	Noted.
387	FirstRand	11.2 (e)	Is there a reason we are singling out GDPR and no other international legislation? Suggestion is to explicitly mention POPIA and ECTA but not specifically GDPR and stating any application international legislation as applicable.	Noted, the examples have been removed.
388	ASISA	11.2(e)	It is not understood why GDPR is specifically referenced and no other similar legislation in other foreign jurisdictions. Foreign privacy legislation will be applicable where a financial institution operates in a foreign jurisdiction regardless of whether a reference is included in the Joint Standard. It is thus suggested that the reference to foreign legislation should be deleted. --- *A financial institution must ensure –* *(e) that all personal information is processed in accordance with the requirements of all applicable legislation, including the Protection of Personal Information Act, 2013 (Act No. 4 of 2013)~~, and where applicable, the General Data Protection Regulation (EU) 2016/679 (GDPR) applicable in the European Union~~.*	Noted, the examples have been removed.
389	FirstRand	General	The section should be amended to simply require that a financial institution's risk frameworks should incorporate requirements for reviews to be conducted to assess compliance with privacy policies, which should include the identification of vulnerabilities in compliance processes that can undermine confidential and sensitive information on its systems.	See response to comment 252. Additionally, when the Authorities assess compliance, specific attention will be given to what is covered in this Standard.
390	SAIA	A financial institution must define, document and implement appropriate measures to protect sensitive or confidential information such as customer personal account and transaction data which are stored and processed in systems; and	Financial institutions are already subject to the requirements of the Protection of Personal Information Act (POPI Act) in this regard. This requirement overlaps with the POPI Act. The Authorities are required to clarify the following:- a) Does the Joint Standard require a different project plan, or can a financial institution leverage off the current project as aligned to the requirements of the POPI Act? b) Should a general obligation to comply with the POPI Act not replace this requirement?	Noted, the intention is not to replace POPIA. However, when the Authorities assess compliance, specific attention will be given to what is covered in this Standard. This Standard must be read in conjunction with other applicable legislations.
391	SAIA	An financial institution must ensure that all personal information is processed in accordance with the requirements of all applicable legislation, including Protection of	The Authorities are required to clarify the reason for the incorporation of the privacy legislation of the EU in the Joint Standard and why only the GDPR is referenced. Further, the requirement may unintentionally extend the mandate of the PA to matters under the supervision of the Information Regulator.	Noted, the examples have been removed.

No	Commentator	Paragraph of the Standard	Comment	Responses
		Personal Information Act, 2013 (Act No. 4 of 2013), and where applicable, the General Data Protection Regulation (EU) 2016/679 (GDPR) applicable in the European Union.		
392	SAIS		No comments.	Noted
392	PSG Konsult		No comments.	Noted
392	Assupol Group		No comments.	Noted
392	Maynard Bester (ISACA member)		No comments	Noted
396	BDO		No comment	Noted
397	HBZ	11.1	No comments	Noted
398	HBZ	11.2	Noted	Noted
399	FEMA		No comment	Noted
400	ECIC		No comment	Noted
401	GENERIC Insurance Company		No comment	Noted
402	JSE		No comment	Noted
403	Ubank		No comment	Noted
404	J Hayden		No comment	Noted
405	SAHL		No comment	Noted
406	BNP Paribus		No comment	Noted
12. Risks associated with products and services				
407	ASISA	12.1	The references to “products” and “services” should be replaced with references to “financial products” and “financial services” as these are the terms defined in the Financial Sector Regulation Act. --- *A financial institution must clearly identify risks associated with the types of financial products or financial services being offered, and formulate security controls, system availability and recovery capabilities, which are commensurate with the level of risk exposure for all operations, including the internet platform.*	Noted, the paragraph has been amended
408	AVBOB	12.1	Would proportionality be applicable if the risks are limited as certain products and transactions are more risky than others e.g. banking transactional facility versus viewing of an insurance policy?	Noted, the Authorities will assess compliance based on the nature, scale and complexity of the financial institution. See paragraph 4.5.

No	Commentator	Paragraph of the Standard	Comment	Responses
409	GenRe	12.1	If these requirements refer to electronic products or services, this should be stated explicitly, else it may be interpreted to go beyond the scope of IT.	Noted, the paragraph has been amended to specify “financial products” and “financial services”.
410	BASA	12.1	BASA seeks clarity on what is meant by "the internet platform". If this refers to a website and web facing platforms then it makes sense, but if it is referring to the internet itself then we suggest that this is not a feasible requirement. The term “internet platform” requires a definition, as such BASA suggests that this term be defined. The identification and management of risks associated with products and services is primarily driven through broader operational risk processes, of which IT risk is but one input/consideration, as relevant. We suggest that – in the context of this Standard – that the requirement in this paragraph be reworded to include specific reference to the consideration of key IT risks in the deployment and maintenance of products and services: “*A financial institution must clearly identify* **key Information Technology (IT)** *risks associated with the types of products or services being offered*, **as relevant**, *and formulate security controls, system availability and recovery capabilities, which are commensurate with the level of risk exposure for all operations, including the internet platform.”* Discretionary FSP’s, with service offerings that extend across external platforms for various JSE authorised investments and collective investment schemes, are contracted via investment management agreements (usually FSCA approved in CAT II Mandates) to cater for segregated risks as the advisor and product supplier. Therefore, it is recommended that scenarios where service level agreements are in place, are indicative of where specific IT related controls under the framework, would reside.	Noted, the paragraph has been amended to make specific reference to IT risks. ‘internet platform’ has been replaced with ‘internet-facing’.
411	FirstRand	12.1	The identification and management of risks associated with products and services is primarily driven through broader operational risk processes, of which IT risk should be a key input/consideration. Suggest the requirement in this paragraph be reworded to include specific reference to the consideration of key IT risks in the deployment and maintenance of products and services: “*A financial institution must clearly identify Information Technology (IT) related risks associated with the types of products or services being offered, and formulate security controls, system availability and recovery capabilities, which are commensurate with the level of risk exposure for all operations, including the internet platform*.”	Noted, the paragraph has been amended to make specific reference to IT risks.
412	BASA	12.2	BASA notes that this creates an obligation to implement controls for systems and infrastructure outside of our members’ management control, including on customers’ private systems. BASA suggests that it should be reworded as “…appropriate reasonable measures…". There are limitations regarding customer protection in this regard. We suggest that the requirements around the protection and the storing of the Encryption Keys between the Financial Institution and the cloud service provider is addressed.	Noted, the Authorities are cognisant of the limitations regarding customer protection; however, the expectation is that the financial institutions should implement appropriate and reasonable measures to protect the customer. Paragraph 11.2 has been amended to include ‘reasonable’.
413	BASA	12.2.a	BASA suggests that this should be rephrased to "associated with its internet-accessible systems".	Noted the paragraph has been amended.
414	FirstRand	12.2 (b)	We suggest rewording this clause as risk may not necessarily arise from the “financial service” itself. 12(2)(b) A financial institution must “*establish appropriate security monitoring systems and processes to detect or monitor risk exposure* ***in relation to*** *the services offered”.*	Noted the paragraph has been amended.
415	FirstRand	12.2 (d)	The way its worded currently might be misinterpreted that the bank will also be responsible for the security of the client’s devices/infrastructure they use to connect to banks online systems. Suggest rewording to indicate the bank only being responsible/accountable for what is under its control e.g.: d) *“implement appropriate measures on the online systems owned and managed by the financial institution in order to protect the customer. Additionally, financial institutions must ensure customer awareness of security measures that are put in place by the financial institution to protect the customers on the online applications/platforms owned and managed by the financial institution*”.	Noted, the Authorities are cognisant of the limitations regarding customer protection; however, the expectation is that the financial institutions should implement appropriate and reasonable measures to protect the customer. The paragraph has been amended to include ‘reasonable’.

No	Commentator	Paragraph of the Standard	Comment	Responses
			While the education of users is ongoing and mandatory to increase awareness, the financial institution is still plagued with instances of online fraud/malfeasance where the customer will blame the financial institution for inadequate communication around security measures. We would therefore need to understand that while ongoing awareness is conducted, customers still remain ultimately liable for information security breaches that persist on hardware/software not controlled/managed by the financial institution. As an example, the bank has been advocating users install antivirus software on any endpoint the customer uses to access online banking This Draft Standard correctly recognises the FSR Act as the "legislative authority" and notes that "In this Standard, 'the Act' means the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) and any word or expression to which a meaning has been assigned in the Act bears the meaning so assigned to it, and unless the context indicates otherwise". The FSR Act refers to a "financial product" or a "financial service". We suggest that all references in this Draft Standard to "product(s) or service(s)" should be replaced with "financial product(s) or financial service(s)".	Noted, the paragraph has been amended to specify "financial products" and "financial services.
416	Masthead	S12.2(d)	*12.2(a) properly evaluate security requirements associated with its internet systems and adopt encryption algorithms which subscribe to well-established and adopted international standards;* Encryption is now prescribed and seems to be a new requirement for FSPs in relation to internet systems. Similar to our previous comments, we agree with the intention of the regulator in enforcing additional security. However, these requirements may have a high cost impact for the FSPs and may not be practical for the majority of smaller FSPs.	Noted, the Authorities will assess compliance based on the nature, scale and complexity of the financial institution. See paragraph 4.3. The paragraph has been amended, Note that 'subscribe' has been replaced with 'aligned' and 'adopted' has been removed.
417	Masthead	S12.2(d)	*12.2(d) implement appropriate measures to protect customers who use online systems to interact with the financial institution and access and transact with its products and services. Additionally, a financial institution must ensure customer awareness of security measures that are put in place by the financial institution to protect the customers in an online environment.* We support the requirement of informing clients around the security measures which protect them. However, this section is unclear in terms of the expectation of level and frequency of information which should be provided.	Noted, the Authorities are cognisant of the limitations regarding customer protection; however, the expectation is that the financial institutions should implement appropriate and reasonable measures to protect the customer. The paragraph has been amended to include 'reasonable'.
418	BASA	12.2.d	As per above comment, online use of the internet system of a product supplier, versus an FSP acting in the advisory capacity or linked investment service providers cater for statutory product supplier accountability under the FAIS Code of Conduct for Administrative and Discretionary FSP's and it is therefore recommended that the standard caters for CAT II FSP's. BASA suggests that more explicit detail should be provided to ensure high levels of security across South Africa's financial ecosystem. For example, it should be mandatory to enforce the use of multi-factor authentication when accessing and / or transaction via internet-accessible systems. BASA notes that awareness of controls to protect customers are required on the institution level, but no awareness of threats that could expose them to risk, fraud or losses, as well as what customers can do to protect themselves. BASA suggests that this could be done on a trend level (not on individual threat level) as a type of awareness campaign, for example if our members are seeing an increase in vishing attacks, or phishing attacks, and this is how to protect yourself against it. BASA is also concerned that this requirement may expose our members' control measures and processes to cyber criminals. BASA also seeks further clarity on what is meant by "Security Measures" with regards to the level of detail required. This Draft Standard correctly recognises the FSR Act as the "legislative authority" and notes that "In this Standard, 'the Act' means the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) and any word or expression to which a meaning has been assigned in the Act bears the meaning so assigned to it, and unless the context indicates otherwise". The FSR Act refers to a "financial product" or a "financial service". We suggest that all references in this Draft Standard to "product(s) or service(s)" should be replaced with "financial product(s) or financial service(s)".	Noted, the paragraph has been amended to specify "financial products" and "financial services.

No	Commentator	Paragraph of the Standard	Comment	Responses
419	AVBOB	12.2 (d)	Ensuring customers' awareness of the security measures imposes too high a standard. Suggest that the wording be amended that the financial institution takes reasonable steps to make the customers aware.	Noted, the Authorities are cognisant of the limitations regarding customer protection; however, the expectation is that the financial institutions should implement appropriate and reasonable measures to protect the customer. The paragraph has been amended to include 'reasonable'
420	Telesure	12.2 (d)	Will a format/ guidance be provided for the way and extent in which a financial institution must create customer awareness in relation to these risks?	Noted, every financial institution will have the latitude to organise its customer awareness programmes.
421	ASISA	12.2(d)	The references to "products" and "services" should be replaced with references to "financial products" and "financial services" as these are the terms defined in the Financial Sector Regulation Act. ---------- *A financial institution must –* *(d) implement appropriate measures to protect customers who use online systems to interact with the financial institution and access and transact with its financial products and financial services. Additionally, a financial institution must ensure customer awareness of security measures that are put in place by the financial institution to protect the customers in an online environment.*	Noted, the paragraph has been amended to specify "financial products" and "financial services.
422	Maynard Bester (ISACA member)	12.2 (e)	ensure that the Software Development Development Lifecycle (SDLC) caters for the security-by-design and privacy-by-design principles (based on best practise and business requirements)	Noted, however this will be added as part of the cybersecurity and cyber-resilient Joint Standard.
423	SAHL		No comment	Noted
424	JSE		No comment	Noted
425	Ubank		No comment	Noted
426	J Hayden		No comment	Noted
427	Maitland		No comments	Noted
428	SAIA		No comments.	Noted
429	SAIS		No comments.	Noted
430	PSG Konsult		No comments.	Noted
431	Assupol Group		No comments.	Noted
432	BDO		No comment	Noted
433	HBZ		Noted	Noted
434	FEMA		No comment	Noted
435	ECIC		No comment	Noted
436	GENERIC Insurance Company		No comment	Noted

No	Commentator	Paragraph of the Standard	Comment	Responses
13. IT programme and/or project management				
437	BASA	13.1	BASA notes that different organisations have adopted different approaches to management of IT programmes and project management and we suggest that the principles should be defined for adoption, lessening prescriptive instruments. For example, there are organisations that have adopted an approach such as the Scaled Agile Framework method which incorporates programme management as a term but quite different from the literal view of programme management methods.	Noted, the authorities acknowledge different types of frameworks. However, the requirements are similar. The financial institution must demonstrate the compliance with the requirement specified under paragraph 13.1.
438	BASA	13.1	BASA suggests that the words “or Policy” be inserted after the word “ Framework”.	Noted. No changes were made as the framework encompasses policy.
439	SAIS	13.1	As stated in the standard: *A financial institution must develop a framework and approach for IT programme and/or project management that incorporates the governance structures, stakeholder engagement, risks and issues management, change control, integration, and* ***cost*** *[emphasis added] and benefit realisation. The framework must be maintained and utilised consistently.* While it is understood that the intention to outsource is to alleviate costs for perhaps smaller financial institutions, the SAIS is of the opinion that this will still be a significant additional cost for smaller authorised users to carry which ultimately will be an additional cost to the end user, the investor. The revenue impact from an operating and human recourses cost perspective *must* be considered, as this will add increased financial pressure on the institution. This would add an extra layer of regulatory costs and complexities which are not aligned to the principles of COFI and will ultimately create additional barriers to entry.	Noted. An impact assessment has been prepared together with this Joint Standard.
440	AVBOB	13.1	Who is envisaged that must approve this? Is it the Governing body?	The framework must follow the financial institution’s internal governance processes.
441	Telesure	13.1	Does the standard consider structures, approaches, methodologies related to the modern agile enterprise? New agile project and programme management practices does not follow the typical PMBOK processes and artefacts. How strict will the standard be applied to specific artefacts as the terminology in the standard only refers to dated project management construct. Example: 1. Scope is no longer fixed; however delivery is timeboxed, but the most valued features are prioritised 2. Change control on the scope of the project is no longer formally documented and signed off. Change control has been replaced with the management of the product and sprint backlog where change is welcomed. Change in priority and scope can take place with the planning refinement of each sprint/release backlog.	Refer to response to comment 437.
441	AVBOB	13 (b)	How independent must the function be from the development function e.g. Quality Assurance (QA) or Production or another Dept or a 2nd line function?	Noted, however this is dependent on differing environment with the financial sector, not every financial institution is following the same methodology. internal governance process should be followed.
443	Telesure	13.1 (h)	Comprehensive documentation has been replaced with technical and business user stories. The days where there was 80-100-page requirements documentation that are signed off doesn’t exist anymore. User stories are reviewed during backlog refinement and accepted by the product owner.	Noted, the authorities acknowledge different types of frameworks. However, the requirements are similar. The financial institution must demonstrate the compliance with the requirement specified under paragraph 13.1.
444	BASA	13.2	BASA suggests that consideration should be given to adding requirements relating to (i) regular review of IT projects and programs to monitor delivery and make informed decisions on material deviations (e.g., course-correct, additional resources, timeline changes); and (ii) regular reporting of material IT projects and programs to senior management.	The Authorities acknowledges that there are different types of frameworks; as such, every financial institution will be assessed on the framework that it utilises.
445	AVBOB	13.2 (a)	This appears to have very detailed requirements. How would non-adherence or contravention of these requirements be monitored and checked?	The governing body is ultimately responsible for adherence and compliance to this Joint Standard. The Authorities will assess compliance through their supervisory processes.
446	FirstRand	13.2 (a)	FIs may have these requirements defined in any of a framework, policy or standard for project management. FirstRand suggests that the statement be amended to cover any of these.	The framework may be incorporated in other documents provided that it is clearly identifiable.

No	Commentator	Paragraph of the Standard	Comment	Responses
			In addition, FirstRand is of the view that not all projects are material and important enough to have such a detailed plan, and hence suggest that the statement be amended to clarify that these requirements be limited to those projects/programmes which are deemed by the FI to be material/significant. .	
447	Hollard	13.2 (a)	I would suggest the substitution of the word "policy" in the statement below with 'framework'. Within a framework there is patterns, OM, processes, procedures, principles, standards. "..establish and implement an IT programme and project management policy that includes, as a minimum.."	Noted. Amendments were made to the paragraph to include policies, procedures and processes.
448	Hollard	13.2 (b)	I would suggest the substitution of the word "policy" in the statement below with 'processes'. "…ensure that its IT programme and project management policy confirms that IT security requirements…"	Noted. Amendments were made to the paragraph to include policies, procedures and processes.
449	Maitland	13.2 (b)	We suggest that the wording be amended as follows: ensure *where feasible, depending on the nature and size of the financial institution,* that its IT programme and project management policy confirms that IT security requirements are analysed and approved by a function that is _independent from the development function	Disagree, these are the minimum requirements for financial institutions to apply. Thereafter consider the application of paragraph 4.5 of the Joint Standard based on the nature, scale and complexity of the financial institution.
450	Masthead	S13(2)(d)	*s13(2)(b) ensure that its IT programme and project management policy confirms that IT security requirements are analysed and approved by a function that is independent from the development function.* As mentioned earlier in this feedback, the implementation of a requirement of independent analysis and approval comes with a potentially high cost impact for smaller independent FSPs who do not have inhouse staff with these skillsets. In view of the broader financial, economic and social environment, this will have a negative financial impact on these FSPs at this time. In our view, this Joint Standard already requires (in s4.3) that financial institutions should apply a proportionate and risk-based approach which is suitable to their organisation size and nature. Therefore, it should be left to the financial institution to decide whether the nature of the business requires and external and independent party to analyse and approve its IT security requirements.	The context of "independent" in this section links back to the requirement in section 9.5 of the Standard.
451	Hollard	13.2 (d)	Does the reference to business management below also include IT management? Some projects are IT4IT. "ensure that, before any acquisition or development of IT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management;"	Noted, the Authorities view IT department as a business function/unit
452	FirstRand	13.2 (f)	The standard only references the risk of unverified changes in this section. There are other risks which are mitigated through having a mirrored pre-prod environment segregated from Production etc. FirstRand therefore suggests the removal of this reference from the statement.	Noted, the paragraph has been amended.
453	BASA	13.2 (f)	BASA notes that Pre-production requirements are never a perfect mirror of production environments as they do not have the same capacity requirements and data is often obfuscated or dummy data used. BASA recommends that a risk-based approach should also be considered in terms of the nature and scale of non-production environments that are required, for example, non-critical and low risk systems need not follow the same standard as high and critical risk systems. BASA suggests that "Segregate" should be added to the definitions clause upfront and then defined to provide clarity as to what is expected.	Noted, the paragraph has been amended.
454	GenRe	13.2 (e)	"…follow an approved methodology for testing and approval of IT systems prior to implementation into the production environment." What does "approved" mean? A best practice standard? Clarity is required.	The paragraph has been amended to indicate that the financial institution must follow 'its' methodology.
455	BASA	13.2 (g)	BASA notes that this is an information risk objective, rather than a programme and/or project management objective. We suggest that it be removed from this section, and in keeping with our other commentary, addressed in a separate standard for information risk, if necessary, rather than incorporated in this Standard.	The paragraph has been removed as it is covered in the cybersecurity and cyber-resilience Joint standard.

No	Commentator	Paragraph of the Standard	Comment	Responses
456	BASA	13.2 (j)	BASA notes that in an organisation using a federated operating model there is no single department responsible for IT and therefore we recommend reference be made to “department/s” and not just ‘department’.	Paragraph has been amended as per the suggestion.
457	SAIA		No comments.	Noted
458	PSG Konsult		No comments.	Noted
459	Assupol Group		No comments.	Noted
460	Maynard Bester (ISACA member)		No comments	Noted
461	BDO		No comment	Noted
462	HBZ		No comments	Noted
462	FEMA		No comments	Noted
464	ASISA		No comment	Noted
465	ECIC		No comment	Noted
466	GENERIC Insurance Company		No comment	Noted
467	JSE		No comment	Noted
468	Ubank		No comment	Noted
469	J Hayden		No comment	Noted
470	SAHL		No comment	Noted
471	BNP Paribus		No comment	Noted
		14. System recovery and business resumption		
472	BASA	14	BASA suggests that the heading be amended to: *IT Resilience and business continuity* BASA suggests that the word "continuity" be amended to "resilience” throughout this section in line with the industry move to the terminology of operational resilience in lieu of traditional Disaster Recovery/Business Continuity Management (DR / BCM).	Noted, the Authorities have amended the heading to ‘IT Resilience’ as well as throughout the Standard
473	BASA	14.1 (a)	BASA notes that with the advent of Operational Resilience (Bank of International Settlements (BIS)) and the principle contained therein for managing resilience for critical services and business processes, as opposed to applications and infrastructure elements, these terms are being replaced with "service level objectives" and "service level indicators". We recommend alignment with the operational resilience thinking, however we are mindful that that the BIS document has not been finalised and suggest that the terms may be included in the Standard once accepted and adopted by the SA authorities.	Noted, the paragraph has been amended to read ‘Define system recovery and business resumption priorities and establish specific Service Level Objectives including RTOs and RPOs for critical services and business processes’.
474	BASA	14.1 (b)	Please refer to BASA’s general comments below, specifically (4). The approach to resilience of systems is fundamentally altered in the adoption of cloud-based models, and requirements such as this are inapplicable in the cloud context. BASA recommends that it should be clarified that the scope of this standard does not extend to cloud computing and/or these requirements will need to be revised to be practically applicable in a cloud context.	Not accepted. The Authorities are of the view that irrespective of whether an institution uses cloud computing or traditional DR site, the principle is the same. Where cloud computing is preferred, different instances should be geographically separate.

No	Commentator	Paragraph of the Standard	Comment	Responses
475	Clientele	14.1.b	In our view “geographically separate” is not very clear and a sensible requirement may differ by business. For instance, we have done detailed analysis of the risks and in Clientele’s case our board is satisfied with the following position: 1. We have 2 data centres which are situated in separate buildings on the same campus. Either data centre can act as the primary data centre at a few hours’ notice. 2. In the event of the whole campus becoming unavailable, we have everything backed up off-site and are able to spin up our systems almost anywhere that we can find hardware. We have a gentleman’s agreement with sister companies that they would provide us with hardware and space in such an event and likewise we would assist them if they suffered such a predicament. This would only be used if we were unable to rent equipment elsewhere immediately after declaring a disaster requiring us to move totally off campus. Given the above, we would recommend the following change to the wording: ‘identify and establish a disaster recovery site that the Board is satisfied is sufficiently separate from the primary site (never in the same building) to enable the recovery of critical systems and continuation of business operations, should a disruption occur at the primary site;’	Noted, in our view “geographically separate” is very clear and a sensible requirement. If the DR and the production sites are within the same proximity, and there are riots and/or disaster in that area, then the financial institution might find it difficult to restore its services.
476	BASA	14.1 (c)	In keeping with the operational resilience concept, BASA suggests that as many organisations are moving away from IT continuity as a discrete discipline toward operational continuity as a holistic approach, IT continuity will be indistinguishable in future and we recommend that this Standard reflects same.	Noted, the Authorities have amended the heading to ‘IT Resilience’ as well as throughout the Standard
477	BASA	14.1 (d)	BASA recommends that the wording be amended to read as follows: “Ensure that the organisation’s business resilience planning and crisis management frameworks adequately address crises and disasters related to IT risk”.	Noted, paragraph has been amended.
478	BASA	14.2	BASA notes that business impact analysis is part of business resilience and/or operational resilience and should not be viewed as a subset of IT continuity management. BASA requests clarity on how often a complete BIA should be conducted. Once a BIA has been established, it should be reviewed at least annually, or when there have been material changes to the associated business process and / or systems.	Noted, the paragraph has been amended to refer to business impact assessment.
479	JSE		No comment	Noted.
480	Ubank	14.6	“A financial institution must test its IT continuity plans periodically. In particular, it must ensure that IT continuity supports critical business functions, business processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually. Various scenarios, including total shutdown or incapacitation of the primary site as well as component failure at the individual system or application cluster level, must be covered in IT continuity tests.” Ubank proposes to change at “least annually” to at “least within 24 months” as it is not feasible for Ubank to test all systems within 12 months. We have mitigation controls as we implemented data replication to our disaster recovery site for critical systems.	Noted, however no changes were made. The Authorities are of the view that annual tests are appropriate for the nature and activities of the financial sector.
481	J Hayden		No comment	Noted.
482	Masthead	S14.4 and S14.5	We propose S14.5 and S14.4 be reordered in order to flow better in terms of the implementation of a policy first, and then the requirements for that policy.	Agreed. The paragraphs have been re-ordered.
483	BASA	14.6	BASA notes that whilst the concept of testing is appreciated, we suggest that a total shutdown of the primary site is not a feasible testing requirement. We are concerned as a full site failover test will certainly introduce more risks to the environment.	Noted, while the Authorities do not support the total shutdown that will introduce adverse risks to the environment, a total shutdown can be considered as a scenario where appropriate.
484	Maitland	14.9	This provision does not seem to consider a work-from-home (WFH) operating model. We require clarity on what the expectation is around a WFH model.	The requirement ensures business continuity. If an institution implements a work-from-home model, it must ensure business continuity.
485	BASA	14.9	A financial institution has a number of premises and follows a risk based approach to disaster recovery and business continuity.	Noted, the paragraph has been amended.

No	Commentator	Paragraph of the Standard	Comment	Responses
			The standard is not clear if this requirement applies only to back up power in relation to IT systems and or IT DR sites or does the requirement apply generically to all premises of the financial institution? BASA suggests the following wording: **“To ensure IT systems continuity management, a financial institution must ensure there is sufficient backup electrical power, a financial institution and must install appropriate backup electrical power facilities consisting of uninterruptible power supplies, battery arrays and/or generators.”**	
486	FirstRand	14.9	A financial institution has a number of premises and follows a risk-based approach to disaster recovery and business continuity for each. FirstRand would like to point out that The standard is not clear whether this requirement applies only to back up power in relation to IT systems and or IT DR sites or does the requirement apply generically to all premises of the financial institution? **Suggested rewording:** 14.9 “*To ensure IT systems continuity management, a financial institution must take a risk-based approach to install appropriate backup electrical power facilities consisting of, where appropriate, uninterruptible power supplies, battery arrays and/or generators*”.	Noted, the paragraph has been amended.
487	FirstRand	14.10	FirstRand requests clarity on what is envisaged by “and so on”, and requests more specific wording be used in the standard to clarify this.	Noted, the paragraph has been amended to read ‘A financial institution must establish a sound IT resilience plan and IT resilience process to ensure the ability to return to a state of normality in the event of severe business disruption’
488	BASA	14.10	BASA suggests that this may duplicated as may already have been addressed in the preceding paragraphs regarding BIAs and establishment of continuity plans.	Noted, the paragraph has been amended.
489	FirstRand	14.12	–This may require that we perform forced failover of networks with our ISP / vendor partners and could cause unnecessary outages. Suggest that this be included as a recommendation rather than “must”. Should only be considered where feasible and does not introduce unnecessary additional risk.	Noted, the paragraph has been amended to allow financial institutions to notify the responsible authority when they are unable to test due to the significant risks.
490	BASA	14.12	BASA notes that there are two different requirements outlined and these should be separated. The one relates to testing of interdependent systems (e.g., several applications that serve a specific business process such as payments); and the second relates to dependencies on third party service providers or vendors. BASA suggests that bilateral or multilateral recovery testing is not a feasible requirement, this is due to the interconnectedness with multiple third parties this requirement will lead to large scale tests involving many third and unrelated parties that will almost certainly lead to service disruption and introduce more risk than it mitigates, particularly where the third parties serve multiple entities in the industry. This is evident in the difficulty Bankserv has in conducting industry-wide failovers. In addition, we recommend that it is desirable to have individual role players perform tests independently as the integration between organisations should be designed and built to be fault tolerant, an attribute that would never be tested if bilateral or multilateral testing approaches were followed.	Noted, the paragraph has been amended.
491	BASA	14.14 (a)	BASA suggests that this requirement should be included with the information security requirements and the comments applicable to those regarding conflation of technology risk and cyber risk are equally applicable to this clause. We note that these talk to the same requirement so only one should be kept, mandating the use of network perimeter controls such as firewalls, Intrusion Detection System (IDS) and Intrusion Prevention System (ISP). In addition, these seem out of place in this section and we suggest that consideration be given to moving them to Information Security section 10, specifically after 10.3(d) which is the requirement for internal network controls, as this talks to the requirement for perimeter and / or external network controls. Please also see our comments at 1.1.(c) herein above.	Paragraph 14.14 has been removed as this will be covered as part of the proposed cybersecurity and cyber-resilience standard.
492	BASA	14.14 (b)	This requirement is a duplication of the business resilience requirements under 14.1, 14.2 and 14.13 and should be incorporated therein.	Paragraph 14.14 has been removed as this will be covered as part of the proposed cybersecurity and cyber-resilience standard.
493	BASA	14.14 (c)	BASA suggests that this requirement should be included with the information security requirements and the comments applicable to those regarding conflation of technology risk and cyber risk are equally applicable to this clause.	Paragraph 14.14 has been removed as this will be covered as part of the proposed cybersecurity and cyber-resilience standard.

No	Commentator	Paragraph of the Standard	Comment	Responses
494	SAIA	A financial institution must establish a sound IT continuity management process to maximise its abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption in line with any existing requirements issued in terms of a financial sector law and applicable to financial institutions;	It is noted that the requirements proposed in the Joint Standard are more prescriptive than those for insurers in the Prudential Standards GOI 3 (Risk Management and Internal Controls for Insurers), specifically the requirements for an Information Technology Policy which should address cyber risk management including having a Cyber Attack Response Plan and the GOI 3.2 (Business Continuity Management). The Authorities are requested to confirm if those Prudential Standards will be revised accordingly.	Paragraph 14.14 has been removed as this will be covered as part of the proposed cybersecurity and cyber-resilience standard. The insurer must follow the requirements of the insurance prudential standards and the requires of other standards that apply to insurers.
495	SAHL		No comment	Noted
496	BNP Paribus		No comment	Noted
497	SAIS		No comments.	Noted
498	PSG Konsult		No comments.	Noted
499	Assupol Group		No comments.	Noted
500	Maynard Bester (ISACA member)		No comment	Noted
501	BDO		No comment	Noted
502	HBZ		Noted	Noted
503	FEMA		No comment	Noted
504	ASISA		No comment	Noted
505	ECIC		No comment	Noted
506	GENERIC Insurance Company		No comment	Noted
507	GenRe		No comment	Noted
15. Outsourcing				
508	BASA	15.1	BASA suggests that the heading be amended to “Outsourcing and **critical Third parties”**	This paragraph has been deleted as outsourcing will in future be dealt with in a separate Joint Standard. Currently the financial institutions must comply with financial sector laws or instruments issued thereunder relating to outsourcing requirements.
509	BASA	15.1	BASA suggests that Government Notice 5 of 2014 covers these requirements which our members are obliged to comply with and therefore we also suggest that it is not necessary to reiterate such in this as controls and measures are in place to ensure compliance with applicable laws referenced here. BASA therefore recommends that this clause be deleted.	See response to comment 508.

No	Commentator	Paragraph of the Standard	Comment	Responses
510	BASA	15.2(i)	BASA suggests that consideration should be given to including the words ‘or policy’ after the word ‘framework’.	See response to comment 508.
511	Telesure	15.2 (a)	Would the assessments being referred to be continuous assessments in accordance with the current principles of outsourcing?	See response to comment 508.
512	AVBOB	15.2 (a)	What are considered to be material activities?	See response to comment 508.
513	FirstRand	15.2 (b)	It is mentioned here that a specific approved policy should be in place for outsourcing IT activities. There is an existing Outsourcing policy and process in place in compliance with the relevant SARB directive, and covers all outsourcing activities, including IT. FirstRand believes that this is sufficient and should not be supplemented by a specific policy for IT or general reference in the standard. Suggest that this statement be amended to “*Outsourcing of IT activities and functions should occur in compliance with G5/2014*”.	See response to comment 508.
514	ASISA	15.2(b)(ii)	The duplicated word should be deleted. --- *A financial institution must, to the extent that such requirement is not in conflict with a requirement in a financial sector law, comply with the following requirements:* *(b) a financial institution must -* *(ii) have a governing body-approved ~~approved~~ policy in place, that would deal specifically with outsourcing of IT activities and functions;”*	See response to comment 508.
515	JSE	15.2(b)(ii)	Duplication of the word ‘approved’.	See response to comment 508.
516	Hollard	15.2 b (ii)	Duplicate approved. “governing body-approved approved policy”- the Insurer already has a Board approved outsource management policy, it would be feasible to include additional sections instead of creating another policy to be approved, monitored and maintained.	See response to comment 508.
517	Hollard	15.2 b (vi) Applicable to 15.2 b (viii) as well.	This should be specifically for outsourced service providers who provide specialised IT Platform services for Hollard. “.require the outsourced service provider to have in place an IT contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures.”	See response to comment 508.
518	Hollard	15.2 b(vi)	This is prescriptive. The group outsource policy that is in line with exiting regulations already includes he requirement for third parties to have recovery processes and plans in place and tested, requesting the vendor to have a framework in place is not necessary.	See response to comment 508.
519	GenRe	15.2 (b) (viii)	This is quite restrictive. Should the insurer have policies, procedures and controls in place that exceed the required level of security by far, all service providers will have to follow this higher level even if they meet the requirements	See response to comment 508.
520	GENRIC Insurance Company	15.2 (viii)	The outsourced service provider controls and procedures should be based on the criticality of the service that it offers.	See response to comment 508.
521	Maynard Bester (ISACA member)	15.2 (b) (ix)	outsourced service provider to provide an annual attestation of service assurance	See response to comment 508.
522	AVBOB	15.2 (b)	How does this differ from requirements for other outsourcing? Would the same definition of materiality as in the outsourcing GOI?	See response to comment 508.
523	BASA	15.3	A financial institution must ensure that it has the ability to recover outsourced systems and IT services within the financial institution’s stipulated RTO and RPO prior to contracting with the service provider. Suggested wording to include a clear requirement for the definition of a stipulated RTO/RPO in contracting as well as attestation to viability of recoverability: “**Stipulated RTO and RPO must be clearly defined in the contracting of an outsourced system and the financial institution must ensure that the service provider’s ability to recover outsourced systems and IT services within the financial institution’s stipulated RTO and RPO has been attested to prior to contracting with the service provider.”**	See response to comment 508.

No	Commentator	Paragraph of the Standard	Comment	Responses
524	Telesure	15.3	Further clarity is needed on this point. Some of the services fall completely wide of the financial institution, the financial institution will not be able to cover this internally as it does not have the capacity to do so. How will this work for say a Telkom or Microsoft? Furthermore, does this suggest that a financial institution must be able to pull in their cloud services in-house within a certain time frame as per their RTO?	See response to comment 508.
525	FirstRand	15.3	The current statement is very broad and can be interpreted as having tested this prior to contracting. FirstRand therefore suggests amending the statement to "*Stipulated RTO and RPO must be clearly defined in the contracting of an outsourced system and the financial institution must ensure that the service provider's ability to recover outsourced systems and IT services within the financial institution's stipulated RTO and RPO has been attested to prior to contracting with the service provider*."	See response to comment 508.
526	BASA	15.4	Shared responsibility models need to be considered in the cloud context. Recovery capabilities will in part be the responsibility of the cloud provider and in part the responsibility of our members. BASA is concerned since cloud service providers will not contract on discrete system RTOs as they almost never take responsibility for the whole stack and in most instances will provide only infrastructure as a service. BASA suggests that consideration should also be given to a requirement to obtain, at least annually, assurance over the continuity capabilities of material outsourced service providers (e.g., in the form of recoverability statements, independent audits, etc).	See response to comment 508.
527	BASA	15.4	BASA suggests that consideration should also be given to the Cloud Computing and the Offshoring of Data (Guidance note G5/2018).	See response to comment 508.
528	Maitland	15.4	This requirement may not feasible when dealing with Cloud Service Providers, as there are prescribed service level agreements for different services.	See response to comment 508.
529	PSG Konsult		PSG Konsult understands section 15 to pertain to the exporting of core competencies that may have a material impact on business functions and impact our ability to manage risk. We do not consider third party technology contracts or vendor IT systems to be outsourcing. Please provide further clarity on the scope of this section.	See response to comment 508.
530	SAIA	A financial institution must ensure that its IT outsourcing is aligned to, and where applicable complies with, any requirements relating to outsourcing contained in financial sector laws.	In a group structure, the IT function and activities are provided to the individual financial institutions within that group from a central group level. The Authorities are requested to confirm if it is intended for such arrangements to fall within the scope of IT outsourcing and therefore subject to the requirements of this section.	See response to comment 508.
531	Assupol Group		No comments.	See response to comment 508.
532	SAIS		No comments.	See response to comment 508.
533	BDO		No comment	See response to comment 508.
534	HBZ		Noted	See response to comment 508.
535	FEMA		No comment	See response to comment 508.
536	Ubank		No comment	See response to comment 508.
537	J Hayden		No comment	See response to comment 508.
538	SAHL		No comment	See response to comment 508.
539	BNP Paribus		No comment	See response to comment 508.

No	Commentator	Paragraph of the Standard	Comment	Responses
16. Assurance				
540.	FirstRand	16.1	Reference is made in this section to an “internal control function” but there is no definition for this. FirstRand requests clarity on which function is being referred to here as not all organisations would have such a function. Once clarity is provided, FirstRand would like the opportunity to provide a response to this section.	Noted, the paragraph has been amended. Please note that the control function referred to on this joint Standard has been defined in FSR Act.
541.	BASA	16.1	BASA recommends that a risk-based approach be stipulated as it is not feasible to provide complete coverage from an assurance perspective.	Noted the paragraph has been amended.
542.	AVBOB	16.1 and 16.2 (a)	This refers to internal control functions but it states that they must have the capacity to independently review and provide objective assurance of compliance with all IT and IT security-related activities Is it envisaged that these existing control functions (risk management, compliance and internal audit) must be expanded / upskilled to include these IT specialists. OR is it rather envisaged that a new IT risk management and governance control function is created?	Noted, the paragraph has been amended. The financial institution needs to have the capacity (existing/expanded/upskilled) to independently review and provide objective assurance on IT. This skill/capacity can also be outsourced
543.	BASA	16.2 (a) and (d)	Points (a) and (d) cover the expectations relating to IT audit. In line with the reference to the "three lines of defence" in 16.1, expectations for second line and first line should be explicitly included in the Standard to be balanced and meaningful.	Noted, the paragraph has been amended. Please note that the control function referred to on this joint Standard has been defined in FSR Act. The Authorities have also included the external assurance providers.
544.	African Bank	16.2(b)	16.2 (b) It’s not clear as to whether this is an assurance activity or operational in nature.	Noted, the paragraph has been deleted.
545.	JSE	16.2(b)	See general comment below in respect of the use of the term ‘organisation’.	Noted, the paragraph has been deleted.
546.	Maitland	16.2 (b)	We submit that this requirement should be based on the nature and size of the financial institution's operations, and not all encompassing as implied in the text.	Noted. the paragraph has been deleted.
547.	BASA	16.2 (b)	BASA suggests that this should be a SLOD/ERM function (where an independent SLOD exists), rather than an Internal Audit function as is implied by the positioning of the paragraph. ERM/ Risk functions are also assurance providers, not only Internal Audit. Audit should be evaluating the effectiveness of controls relating to incidents and problems, not analysing individual incidents and the lessons learned. This may influence the independence of Internal Audit if they get involved in the incident management process. BASA recommends that this should be included in IT Operations (section 9), unless the expectation is that these activities must be independently performed and if so then this should be explicitly stipulated as such in the requirements. There is also a view is that IT assurance does not necessarily imply the independent audit function. In a combined assurance model, 1st, 2nd and 3rd line all can undertake assurance work, but the degree of reliance will vary depending on which line does the assurance. 1st line self-assessments are seen to be a measure of assurance, but less reliance will be placed on this compared to an exercise undertaken by a independent audit function.	Noted, the paragraph has been deleted.
548.	Maitland	16.2 (c)	We submit that this requirement should be based on the nature and size of the financial institution's operations, and not all encompassing as implied in the text.	Disagree. The Joint Standard covers the minimum requirements for IT Risk. The provisions of paragraph 4.5 of the Joint Standard will thereafter apply in terms of the nature, scale and complexity of the respective financial institution.
549.	AVBOB	16.2 (c)	Is it envisaged that the formal change management process be governing body approved? Or would management approval suffice?	The Joint Standard has been amended to take into consideration the comment.
550.	BASA	16.2 (c)	BASA suggests that this should be a SLOD function (where an independent SLOD exists), rather than an Internal Audit function. ERM/ Risk functions are also assurance providers, not only Internal Audit. BASA notes that the Audit function should be evaluating the effectiveness of controls in the new/ changed processes, not assisting management in designing and implementing controls to mitigate risks due to changes in the environment or determining whether risks are adequately mitigated. That should be with a SLOD/ ERM function. BASA is also concerned that this may influence the independence of Internal Audit. BASA suggests that further clarification be provided in terms of how the requirements are documented. Clause 16.2 (b) and (c) specifically could result in	See response to comment 548 above,

No	Commentator	Paragraph of the Standard	Comment	Responses
			independence issues for Internal Audit if they are operationally too close/involved. The two sub-paragraphs appear to imply a certain level of operational involvement in incidents and process changes for Internal Audit, rather than pure audit oversight over control adequacy and effectiveness in those areas (based on their positioning between 16.2(a) and (d) which specifically references Internal Audit). BASA recommends that this should be included in IT Operations (section 9), unless the expectation is that these activities must be independently performed and if so then this should be explicitly stipulated as such in the requirements.	
551.	Maitland	16.2 (d)	We submit that this requirement should be based on the nature and size of the financial institution's operations, and not all encompassing as implied in the text.	See response to comment 548.
552.	J Hayden		The internal control functions of a financial institution, including the three lines of defence, must, following a risk-based approach, have the necessary knowledge, skills, qualifications (E.g., CISA, ISAP (SA)), and capacity to independently review and provide objective assurance of: a. the IT risk management arrangements, b. the effectiveness of the IT control environment, c. the performance of the institution's IT goals, strategies and objectives, d. the conformance with the institution's policies and procedures, and e. the compliance with external requirements.	Noted, however the Authorities do not subscribe to any frameworks, qualification bodies, etc
553.	SAIA		No comments.	Noted
554.	SAIS		No comments.	Noted
555.	PSG Konsult		No comments.	Noted
556.	Assupol Group		No comments.	Noted
557.	Maynard Bester (ISACA member)		No comment	Noted
558.	BDO		No comment	Noted
559.	HBZ		Noted	Noted
560.	FEMA		No comment	Noted
561.	ASISA		No comment	Noted
562.	FEMA		No comment	Noted
563.	SAHL		No comment	Noted
564.	BNP Paribus		No comment	Noted
565.	Ubank		No comment	Noted
566.	GENERIC Insurance Company		No comment	Noted
567. 3	GenRe		No comment	Noted
			17. Reporting	
568.	FEMA	17.1	Further clarity is required as it relates to the form and manner in which a material incident must be reported to the FSCA and PA.	Noted, the reporting template will be published for comment.
569.	FEMA	17.1	It is not understood why a financial institution that is only being supervised by one financial sector regulator (a responsible authority as defined in the Financial Sector Regulation Act) should notify both the Authorities of any material systems failure etc. A financial institution should only be required to notify the responsible authority for a financial sector law. It is proposed that paragraph 17.1 of the Joint Standard should be amended accordingly. --- *A financial institution must, unless such a reporting obligation already exists in another financial sector law, notify the ~~Authorities~~ responsible authority, in the form and manner determined by the Authorities, of any material systems failure, malfunction, delay or other disruptive event, or any breach of IT security, integrity or confidentiality, within 24 hours of classifying the event as material.*	Noted, the Authorities have amended the Joint Standard accordingly.
570.	FirstRand	17.1	Reference is made to the PA's directive 2 of 2019, to the following sections within:	Noted, the paragraph has been amended.

No	Commentator	Paragraph of the Standard	Comment	Responses
			Directive 2/2019 issued in terms of section 6(6) of the Banks Act 94 of 1990. Reporting of material technology and/or cyber incidents 1.6.2 An 'IT incident' is defined as an event, occurrence or circumstance that is not expected or planned as part of the normal operations of a bank and has an effect of disrupting the normal operations of the bank's IT systems or services. 1.6.3 A 'cyber incident' is any observable occurrence in an information system that (i) jeopardises the cybersecurity of an information system or the information processed, stored or transmitted by the system; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. 2.1.4 Notify the, as soon as practically possible but not later than one day, following the discovery of a material IT and/or cyber incident. FirstRand recommends that section 17.1 in the standard be amended to align with the above definitions so that there is no misunderstanding between the two documents.	All reporting in terms of IT incident reporting will now be done in terms of this joint Standard. Cyber incident reporting will be covered under cybersecurity and cyber-resilience joint Standard.
571.	JSE	17.1	We recommend that the Authorities provide clarity in respect of the 'material' reporting requirement ('within 24 hours of classifying the event as material') provided for in this draft Standard in relation to the 'significant event' requirement provided for in the FSCA's *Notice to Market Infrastructures to Report Significant Events to the Registrar*, dated 20 June 2017, ('within 48 hours of becoming aware of the significant event'). We have assumed the Standard would prevail and the Notice will be withdrawn, however, for the sake of clarity, we would appreciate confirmation of our assumption.	The Authorities will determine the form, manner and period for reporting. It may necessitate the withdrawal of other instruments. This will be consulted on in due course.
572.	Hollard	17.1	Would it not be more appropriate to report material failures that were not recoverable or acceptable? (In IT the VPN will have material impact. If it drops twice in one month resulting in some disruption, do we need to report this? If this is the case, then we will have to report every single P1 incident monthly.) If we are resolving non-recoverable material failures, it would be ideal to report it in 7 working days. From the standard document: "A financial institution must, unless such a reporting obligation already exists in another financial sector law, notify the Authorities, in the form and manner determined by the Authorities, of any material systems failure, malfunction, delay or other disruptive event, or any breach of IT security, integrity or confidentiality, within 24 hours of classifying the event as material."	The requirement is that all financial institutions will need to report material IT incidents within 24 hours of classifying such as material.
573.	Brightrock	17.1	Please provide clarity on the form and manner of the reporting.	Refer to respond to comment 571.
574.	Maitland		No comment	Noted.
575.	Masthead	S17.1	*A financial institution must, unless such a reporting obligation already exists in another financial sector law, notify the Authorities, in the form and manner determined by the Authorities, of any material systems failure, malfunction, delay or other disruptive event, or any breach of IT security, integrity or confidentiality, within 24 hours of classifying the event as material.* We propose that in view of the content of this section, the reporting requirements under section 6.3(c), which are more general in nature, can be removed.	Disagree. Paragraph 6.3(c) deals with reporting to the Authorities of contravention of this Standard, whereas this requirement relates to specific instances where there is a material risk to consumers that requires urgent reporting to the Authorities. The rationale for these two requirements are therefore different.
576.	Telesure	17.1	The term 'material systems failure' is not defined. Will the financial institution be the one to define and determine the materiality?	Noted, the paragraph has been amended and relevant definitions are included
577.	BASA	17.1	BASA suggests that consideration should be given to changing the heading to "Reporting of Material Incidents", to align with the expectations set out in D2/2019: Reporting of material information technology and/or cyber incidents. BASA suggests that the reporting requirements for material incidents / data breaches and to which Regulatory body this information needs to be submitted to should be specified. BASA would also appreciate clarity on what is meant by "delay". BASA understands that this section currently envisions reporting along the lines of Banks Act Directive 2/2019: Reporting of material information technology and/or cyber security incidents and the definitions and requirements as set out in it. Given that this Standard will be applicable across multiple sub-industries within the Financial Sector, the risk exists that different industries may have different reporting requirements in terms of material IT incidents. Where an organisation operates across multiple industries (e.g., banking and insurance), a misalignment in different industry-specific legislation or regulation may result in grey areas, duplication of reporting, or misinterpretation of requirements. BASA suggests that more clarity be provided in terms of either directly defining material IT incidents and the reporting requirements or	Noted, the paragraph has been amended. All reporting in terms of IT incident reporting will now be done in terms of this joint Standard. At some point D2/2019 will be repealed.

No	Commentator	Paragraph of the Standard	Comment	Responses
			referencing the specific legislation/ regulation per industry (e.g., Directive 2/2019 for Banking) placing a requirement on financial institutions to report material incidents. BASA is also concerned that the current wording creates a grey area that can result in multiple different definitions, interpretations and responses with regards to material IT incidents should future legislation be introduced.	
578.	BNP Paribus	17.1	17.1 - Is there any standard template to report the material impact to SARB?	Refer to response to comment 571.
579.	SAIS	17.2	As stated in the draft, "The Authorities may, through ongoing supervisory review and evaluation processes, request for specific information or reports as well as assurance in terms of compliance with this Standard." It is not clear from this clause which authority, will be performing the review. It must be clarified if the authority mentioned will be the FSCA, the Prudential Authority or whether this will this be delegated to the exchanges. Authorised users are already required to comply with robust IT requirements, as mandated by the exchanges, in order to ensure effective risk management. The implementation of the measures as set out in this draft will result in substantial additional IT costs, which will not be practical or inclusive and will negatively impact the market. It is recommended that further consultation be undertaken in order to understand the full impact of these requirements, specifically for authorised users that are FSPs.	This is a Joint Standard. Please refer to the definition of "Authorities". The information can be requested by either the FSCA or the PA. It is not, at this stage, the intention to delegate this function to the exchanges. Please refer to paragraph 4 of the Statement of Need. It is not clear from the comment to what extent the existing IT requirements, mandated by the exchanges, differ from the requirements of this Standard and the extent to which implementation of the provision of this Standard will have a further cost implication. It is not clear why this information was not provided in this consultation process.
580.	BNP Paribus	17.2	17.2 – Is the regulator expecting compliance assurance to this standard through Self-Assessment or should an independent external Auditor perform the assessment? What is the compliance assurance reporting requirements for the regulator? What is the frequency? Please clarify.	The Authorities are expecting financial institutions to perform self-assessments. In addition, independent review will be required from assurance providers. Independent review has been defined in this joint Standard.
581.	BASA	17.2	BASA suggests that the word "*Regulatory*" be inserted before the word 'Authorities' wherever reference is made to 'the Authorities".	Not accepted. The term 'Authorities' is defined in this joint Standard.
582.	PSG Konsult		We submit that the 24-hour reporting window for reporting material events is not feasible and further, does not align with other regulation such as POPIA and the Cybercrimes Act. We recommend an alignment with related regulation.	The 24 hours has been removed from the Joint Standard and will be determined in the reporting return.
583.	Assupol Group		We propose reporting within a "reasonable period" to enable the institution some time to gather enough information to be included in the report. 24 hours may not be sufficient. An extended period is recommended. "Reporting 17.1 A financial institution must, unless such a reporting obligation already exists in another financial sector law, notify the Authorities, in the form and manner determined by the Authorities, of any material systems failure, malfunction, delay or other disruptive event, or any breach of IT security, integrity or confidentiality, within 24 hours of classifying the event as material."	See response to comment 582.
584.	SAIA		No comments.	Noted
585.	Maynard Bester (ISACA member)		No comments	Noted
586.	BDO		No comment	Noted
587.	HBZ		No comment	Noted
588.	ECIC		No comment	Noted
589.	GENERIC Insurance Company		No comment	Noted
590.	Ubank		No comment	Noted
591.	J Hayden		No comment	Noted
592.	SAHL		No comment	Noted
593.	GenRe		No comment	Noted

No	Commentator	Paragraph of the Standard	Comment	Responses
		GENERAL COMMENTS		
594.	SAIA	Governance Arrangements	a) For smaller insurers and other financial institutions, even those within a larger group of companies, the level of governance should be aligned to the size, complexity, and risk of the business. It is respectfully acknowledged that although section 4.3 provides that the requirements of the Joint Standard must be implemented in accordance with the nature, size, and complexity of a financial institution, this is not reflected further within the Joint Standard, where the requirements prescribed do not adequately reflect this intended application. b) The Authorities are requested to clarify if a dedicated board committee for IT risks must be established.	The Authorities are of the view that reflecting this under the application of the Standard is sufficient. While it is not a requirement to have a separate IT Board committee as this can be incorporated in existing risk oversight structure, the Authorities are of the view that this is recommended
595.	SAIA	Group Structures/ Designated Insurance Groups	For group structures and insurance groups, some requirements may be best served at a central group level such as privacy and cybersecurity requirements, but others may need to be managed at an entity level for alignment of business applications with the specific entity strategy. It is recommended that the Standard considers a split governance, whilst still assuring accountability, approach.	Each financial institution captured by this Joint Standard must be able to prove compliance with the requirements on institution-specific risk whether it is captured at an institution level or at a group level.
596.	SAIS	Single View	Part of the definition of a financial institution is that "…a market infrastructure registered in terms of the Financial Markets Act 2012 (Act No. 19 of 2012); a discretionary FSP as contemplated in the Code of Conduct for Administrative and Discretionary FSPs, 2003; and an administrative FSP as contemplated in the Code of Conduct for Administrative and Discretionary FSPs, 2003, published in terms of the FAIS Act". As such, the SAIS is of the opinion that this standard will not be applicable to all authorised users. However, it is important to note that the majority of authorised users are also FSPs and there will be a direct impact on these authorised users. The SAIS has therefore provided comment, in relation to this standard, from this perspective and with this context in mind The SAIS would request more consultation and clarity regarding the applicability of the standard in cases where an authorised user is also a FSP, as licenced under FAIS. If there is to be alignment to the principles of COFI, there is need for clarity on the overall requirements and a consistent, single view of all regulatory requirements in order to ensure that there is no duplication of costs. There must be a single set of requirements that must be streamlined to ensure compliance with the principles of COFI and the FMA review etc.…This single set of requirements must be clear, practical and duly considered, so as to ensure that all participants are treated fairly. This will ensure a consistent regulatory approach and a level playing field that is regulatory compliant and cost effective across participants. *It is imperative for authorised users not to be penalised by having to adhere to duplicate regulation.*	Agree.
597.	SAIS	Unquantified Layered Friction Costs	The SAIS and by extension the Financial Market participants (Authorised Users) that the SAIS represents, are largely concerned with the unquantified, layered friction costs, which will be added by these requirements. The proposed IT risk measures, whilst robust, will create a heavy additional cost for authorised users to carry. This will in effect be a barrier to entry and non-inclusive, which in itself is against the principles that the proposed COFI Bill is trying to achieve. These requirements will greatly affect the authorised user's operation costs. It is noted that these costs will have to be passed on to the investor, in some form or the other. The SAIS is of the opinion that this requirement will have a negative impact on authorised users and seriously impact some authorised users' ability to conduct business. This is even more critical given the effect of the COVID-19 global	The Authorities would welcome the impact assessment performed by SAIS. However, the requirements in Joint Standard are minimum requirements for IT Risk Management.

No	Commentator	Paragraph of the Standard	Comment	Responses
			pandemic. It is highly unlikely that the industry will be able to absorb the aggregated costs that may ultimately be passed down to it, even if a regulated IT environment is beneficial for the industry and protects investors. Given the above, the SAIS is of the opinion that an in-depth impact analysis is imperative. It is critical to quantify the cost to the authorised user and in turn, the ultimate beneficial owner/investor who invests through these multiple investment avenues, which may just carry the burden of these costs downstream. It is important to be cognisant that the financial market participants view the proposed IT risk management requirements as an additional layer of costs i.e. authorised users will pay to regulate and manage risk for fair outcomes for the investor. The concern, specifically, is in respect of the cumulative effect of the regulatory levies and fees which will be passed on, by supervised entities, to participants, investors, and financial consumers. The SAIS is of the opinion that it is essential that the finalisation of the COFI Act, the revision of the Financial Markets Act (FMA) and the introduction of Codes of Conduct must be completed together with the finalisation of such additional requirements. This would provide for a holistic view of the regulatory and IT architecture and an understanding of the end-to-end regulatory frictional costs and framework impacting the market.	
598.	SAIS	Self-Regulating Organisation (SRO) Model	In general, the SAIS reiterates that the finalisation of the COFI Act and the FMA review is vital, as further clarity is required in respect of the role of SRO's and the delegation of duties by the regulator i.e. the FSCA. The costs, processes and procedures for authorised users must create equitable and level playing fields. The SAIS believes that regulatory and IT risk management costs payable should be commensurate to the intensity of regulation and supervision required and should be proportional to the nature, scale and complexity of regulatory risks present. Regulation should not be the cause of additional costs and regulatory burdens that participants cannot incur. This will severely and negatively impact business, due to increased operation costs and human capital.	Noted. See paragraph 4.5
599.	SAIS	Further Engagement	All stakeholders should continue engaging the relevant role players to ensure that the protocols, processes, and desired outcomes are obtained. In finalising the IT risk management requirements to be imposed on financial institutions, a practical view of the impact on all market participants must be analyzed and the industry must be further consulted in the finalisation process.	Noted. Please refer to paragraph 4.3 of the Statement of Need as to the purpose of this consultation process.
600.	SAIS	Conclusion	The SAIS has reviewed the proposed IT Risk Management requirements and foresees that these will have a significant impact and cost implications to authorised users. The SAIS is of the opinion that the introduction of these requirements must align to the ultimate objective of the COFI Act and should not have the unintended consequences of creating complexity, fragmentation and additional compliance burdens as well as other costs, to regulated entities. It is of the utmost importance to align legislation as well as additional regulatory requirements i.e. IT Risk Management. Who the IT Risk Management framework is intended to affect must be clearly stipulated. All authorised users already have to account for stringent IT Risk Management measures, imposed by the Exchanges and should not have to create dual structures and costs for those authorised users that are FSP's. This will ensure that there is fairness and equity for all market participants and financial institutions, while ensuring that the necessary regulations are in place that promote transparency, fairness, competition and the protection of the integrity of the South African financial markets. Additional engagement and analysis of empirical evidence, to determine the friction costs caused by implementing these IT Risk Management requirements is vital. A significant increase in the cost of regulatory compliance and mandatory IT Risk	This is a Joint Standard. Please refer to the definition of "Authorities". The information can be requested by either the FSCA or the PA. It is not, at this stage, the intention to delegate this function to the exchanges. Please refer to paragraph 4 of the Statement of Need. It is not clear from the comment to what extent the existing IT requirements, mandated by the exchanges, differ from the requirements of this Standard and the extent to which implementation of the provision of this Standard will have a further cost implication. It is not clear why this information was not provided in this consultation process.

No	Commentator	Paragraph of the Standard	Comment	Responses
			Management could lead to unintended and dire consequences for the South African capital markets. The SAIS is of the strong viewpoint that well-regulated financial markets are essential however, the benefits should not be outweighed by the regulatory burden and should be balanced with the cost of implementing these regulatory requirements. The SAIS would request more consultation and clarity regarding the applicability of the standard in cases where an authorised user is also a FSP, as licenced under FAIS. If there is to be alignment to the principles of COFI, there is need for clarity on the overall requirements and a consistent, single view of all regulatory requirements in order to ensure that there is no duplication of costs. There must be a single set of requirements that must be streamlined to ensure compliance with the principles of COFI and the FMA review etc.…This single set of requirements must be clear, practical and duly considered, so as to ensure that all participants are treated fairly. This will ensure a consistent regulatory approach and a level playing field that is regulatory compliant and cost effective across participants. *It is imperative for authorised users not to be penalised by having to adhere to duplicate regulation* The SAIS looks forward to closer and more collaborative working relationship to find optimal solutions for the industry.	
601.	PSG Konsult		No comment	Noted
602.	Assupol Group		No comment	Noted
603.	Maynard Bester (ISACA member)		No comment	Noted
604.	BDO		The standard should consider including specific and detailed guidance on data governance and or reference in detail to the BCBS239 principles. While we acknowledge that data governance may fall under the IT strategy and IT risk framework, there is a need to standardise and inter-link this standard to the data governance/ BCBS239 principles which will ensure that the foundation for newly implemented technologies are being appropriately managed and governed.	We note the comment, this joint Standard is about IT risk management and governance. Please also note that, the proposed joint standard is meant to apply to other financial institutions. The Authorities may in future consider incorporating the BCBS239 principles into appropriate and relevant instruments.
605.	HBZ		No comment	Noted
606.	FEMA		No comment	Noted
607.	ASISA	Title of the Standard	The Draft Joint Standard does not only address IT Risk Management. It also sets requirements for an IT strategy, IT operations, Information Security etc. It is thus proposed that the Authorities consider changing the title of the Standard to *"INFORMATION AND TECHNOLOGY GOVERNANCE"*. This title will be more reflective of the all-encompassing requirements included in the Standard. While IT Governance is the generally used term, King IV specifically refers to information **AND** technology governance to recognise that information and technology overlap but are also distinct sources. It is proposed that the same reference should be used in the Joint Standard.	We agree in principle. The title of the joint Standard has been changed to IT risk management and governance
608.	ASISA	Objectives and key requirements of Joint Standard – Information technology risk management	It is suggested that the paragraph should be rephrased to improve the reading thereof. ---------- ***Objectives and key requirements of Joint Standard – Information and technology ~~risk management~~ governance*** *This Standard sets out the principles for ~~information technology (IT) risk management~~ information and technology governance and requires that financial institutions must comply with sound practices and processes in managing IT.*	Accepted the paragraph will be aligned to the new title of the joint Standard which is IT risk management and governance

No	Commentator	Paragraph of the Standard	Comment	Responses
609.	ASISA	General	This standard is a positive step for financial services in South Africa and it will assist in improving IT governance.	Noted.
610.	ASISA	Structure of Joint Standard	Some ASISA members are of the opinion that the Joint Standard effectively covers IT risk management and guidance on controls and that the Joint Standard will be easier to read and implement if the Joint Standard was restructured by separating guidance on controls into an annexure to the Joint Standard. The paragraphs providing guidance on controls are viewed to be the following: 6. IT Strategy 9. IT Operations 10. Information Security 12. Risks associated with products and services 13. Part of IT Programme and/or project management 14. System recovery and business resumption Outsourcing	The Joint Standard contains principles and requirements. Guidance is captured in a Guidance Notice.
611.	ASISA	Engagement	ASISA, on behalf of its members, kindly requests to engage with the Authorities on its members' comments as set out above and will appreciate an indication when the Authorities are ready to do so.	Noted, Authorities will consider meeting with industry bodies
612.	African Bank		As African Bank we generally agree with the proposals articulated in the IT Risk Management standard. However, we suggest that there should be reconsideration around the sequence and presentation of some of the IT process covered. Please refer to below points for some sequential and structural observations we made: • "Sensitive and confidential information" generally forms part of "Information Security" however in the proposed IT Risk standard the topic is separated. This creates an impression that "Sensitive and confidential information" is seen as a separate process from Information Security. • "Access Management" which generally forms part of IT Operational management process is covered under "Sensitive and confidential information". It is unclear why it is not presented as a stand-alone process or perhaps have it covered under section 9 "IT Operation" so it forms part of change management, incident management, capacity management etc. • Other process critical to IT risk management are not as explicit like others in the standard i.e. Enterprise and solution architecture	The Information Security has been moved to the Joint Standard on Cyber Security and Resilience, however high level risk management requirements are still covered in this Joint Standard. Access also relates to IT Risk Management but access management is covered in detail in the cybersecurity and cyber resilience Joint Standard. Enterprise Architecture is unique to each financial institution and the risks derived therefrom must be managed through the IT Risk Management framework.
613.	ECIC		Generally, the standard is well written. More consideration or guidelines can be given to risks associated with cloud services and cybersecurity given that these present new opportunities and challenges for Financial Institutions.	Noted. A Cybersecurity and cyber-resilience Joint Standard was released for comment in December 2021.
614.	GENERIC Insurance Company		GENRIC is content with the standard except for the issue raised under 15.2 (viii) outsourcing.	Noted
615.	FirstRand	1st page	Commentary here relates to the statement below, contained within the Objectives section in the first page of the standard. "This standard sets out the principles for information technology (IT) risk management that financial institutions must comply with sound practices and processes in managing IT" The above statement does not read as being complete. FirstRand suggests we change to "*This standard sets out the principles for information technology (IT) risk management that financial institutions must comply in line with sound practices and processes in managing IT*", as reflected in Annexure A which the PA circulated together with this standard.	Noted, the paragraph has been amended.
616.	FirstRand	General	The minimum requirements are very detailed, will there be an exceptions process in cases where we are unable to meet the minimum requirements as all requirements will not be achievable all the time? If there is to be such a process, then FirstRand recommends that only material deviations be reportable.	The Authorities expect the financial institutions to comply with the requirements of this joint Standard.
617.	FirstRand	5.2 From Annexure B- Statement:	Due to the varying sizes of the different FIs, FirstRand suggests that the standard should include consideration with regards to implementation of the requirements based on the nature and size of the financial institution's operations.	Paragraph 4.3 covers this matter.

No	Commentator	Paragraph of the Standard	Comment	Responses
618.	JSE	Definitions; 7.3(a); 10.3(a); 16.2(b)	The terms “enterprise”, “organisation” and “business environment” are used interchangeably in the draft Standard. We recommend that one term is used consistently throughout the Standard.	Disagree. In the context that it was used, “business environment” does not mean “enterprise” or “organisation”.
619.	Ubank		No comment	Noted
620.	Dotsure	Overall Standards	We have reviewed the provisions of this joint standard and have no concerns regarding these requirements. We require an indication from the Authorities on whether they intend to publish any practice/guidance notes on these IT Risk Joint Standard before their implementation.	The Authorities do not intend to publish any practice/guidance notes to support this joint Standard at present. The Authorities expect the financial institutions to comply with the requirements of this joint Standard
621.	J Hayden		**No comment**	Noted
622.	Brightrock		**No comment**	Noted
623.	Masthead		We agree that increased security and IT Risk management requirements may be required for complex and large financial institutions who offer complex products or services, or who make use of complex IT solutions and systems. However, these requirements are currently made generally applicable and will have a high cost and resource impact on smaller independent FSPs. We further note that, in particular for smaller FSPs, while the Joint Standard is prescriptive and onerous, it is not in all instances clear what risks are being managed or the intended purpose for which the requirements are being implemented. Asked simply, what “evil” has occurred, needs to be stamped out, and that justifies these requirements. Based on paragraph 2 of the Statement issued by the Authorities in order to fulfil their obligations in terms of sections 98(1) and 103 of the FSR Act, it looks like nothing has happened, but that the requirements are being put in place “just in case” something happens?	Please refer to paragraph 4.3 of the Standard. Please also refer to the Statement of Need which describes sufficiently the risks that the Authorities seek to address.
624.	SAHL		No comment	Noted
625.	Ninety-one		Many Financial Institutions form part of group structures, where shared infrastructure and services are used across the businesses including in the IT environment. It is not clear from the Standard that shared infrastructure, systems, and processes may be used in the instances where Financial Institutions form part of a group, as long as it is documented.	The financial institution must comply with the requirements set out in the Standard. The manner of compliance is not prescribed.
626.	BNP Paribus		No comment	Noted
627.	BASA		BASA notes in the Standard that where it is not feasible to implement one of the requirements due to for example resource and or budget constraints, clarity is sought on whether it would be acceptable for our members’ EXCO to accept the risk.	The Authorities expect the financial institutions to comply with the requirements of this joint Standard.
628.	BASA		BASA suggests that this Standard appears to conflate technology risk, information risk, cyber risk and information security and that these are discrete topics, and there are existing regulatory instruments addressing the latter three categories, and therefore they need not be covered in this Standard.	While we acknowledge that these topics have been covered in this Standard, however it is sometimes not possible to separate. In instances where possible, we have separated the topics.
629.	BASA		BASA notes that there are multiple clauses requiring adherence to other laws and regulations. This appears unnecessary as these are already mandatory obligations and will simply add to the cost of compliance with this Standard without any discernible incremental benefit and we recommend that same should be removed from this Standard.	This is made to ensure that the requirements are read together.
630.	BASA		BASA notes that cloud computing is not comprehensively addressed in this Standard, and it would not be desirable to replicate what is already well addressed in the Prudential Authority’s directive and guidance note on cloud computing and offshoring of data. However, clearer reference should be made to this in this Standard, as the practical approach to IT risk management is somewhat different for cloud computing and there is ambiguity regarding the applicability of this Standard’s requirements to cloud computing environments.	Noted, Cloud computing regulation has been issued to the banking industry and the same will be replicated in a form of a prudential/joint Standard to the sector Furthermore, it should be noted that irrespective of whether an institution uses cloud computing or its own datacentres, the principles are the same.
631.	BASA		The contents of this standard are largely based on the management of IT Risks in environments where IT assets are hosted on the Financial Institution’s premises. However, the migration of digital services to cloud based platforms across industries is accelerating. The standard needs to be advanced to take a firm stance on the management of IT Risks in cloud based environments.	Noted, however irrespective of whether an institution uses cloud computing or its own datacentres, the principles are the same.

No	Commentator	Paragraph of the Standard	Comment	Responses
632.	BASA		Reasonable timelines would be required to implement the requirements for the respective Financial Institutions to comply, being a minimum of six to twelve months from the effective date of the Standard.	The Authorities have provided 12 months for financial institutions to prepare for the implementation date of the Joint Standard once it has been published.
633.	AVBOB		It appears that the draft standard intends to address at least two key areas being visibility and independence. Visibility or line of sight being what is happening in IT and do management and the Board have a firm handle on what is happening in IT due to the technical nature of the discipline. Independence in the sense of the Board getting independent assurance of the effectiveness of the IT function. The standard appears at times to conflate these two end goals.	Not accepted. The visibility and independence are not conflated, however, the joint Standard seeks to ensure visibility and independence.
634.	AVBOB		It appears that what is being envisaged here is similar to the control functions insurers must have in place with a head of control i.e. risk management, compliance, internal audit and actuarial. Like a head of control for IT risk management and governance. Could this be clarified?	The control functions play a role with regard to the lines of defence in overall management of risks.
635.	Clientele	9	Many of the sub-sections of 9 (especially subsection 3) contain adjectives and adverbs describing that something should be effective or prevent some event. If a previously effective process breaks down for some reason it should not be a contravention of the standard. If the event to be prevented occurs despite a good process being implemented, it should not be a contravention of the standard. Some of the terms used in section 9 seem to be more absolute in nature, and less risk-based. Usually a standard defines the absolute inputs required in the hopes of achieving a standard outcome. When the outcome is defined in the standard instead of clear absolute inputs, then various different solutions to the requirement may be implemented by various institutions and any failure (even if it is due to an extreme scenario) could be seen as a contravention. I am certain this is not the intention of the standard, but rather to require all institutions to implement good solutions and processes.	The Authorities are of the view that this joint Standard contain minimum requirements.
636.	GenRe		Information Technology Risk Management is subject to changes in technology and security concepts, where the latter is in part the result of changes to the threat landscape. There is a risk that the Information Security prescriptions in the Joint Standard are too detailed to allow financial sector institutions to respond optimally to such changes in technology and security concepts. As a result, there is a risk that this highly prescriptive framework results in a suboptimal level of cyber security, where suboptimal means less security for the allocated amount of financial and human resources. Two examples of changing concepts in cyber security are (1) the migration of many firms from a maturity-based approach to a risk-based approach, and (2) the rise in prominence of a zero trust security concept in the wake of heightened supply chain risk.	The Authorities acknowledges that the threat landscape will evolve over time and as well as the response. However, minimum requirements are necessary. Requirements regarding cyber security will be covered in a separate Joint Standard. .
637.	GenRe		This standard applies to local insurers. However, it does not seem to consider reinsurers that have an international parent company, who manages Information Technology and Information Technology Risks on a global level for all companies within the group.	Each financial institution captured by this Joint Standard must be able to prove compliance with the requirements on institution-specific risk whether it is captured at an institution level or at a group/global level.

Table 4

Area	Summary of comment	Response from the Authorities
Commencement of the Joint Standard	No comments were provided on the commencement of the Joint Standard.	The Joint Standard will come into effect approximately 12 months after date of publication in order for financial institutions to prepare for compliance with the Joint Standard
Legislative Authority	Clarification on the 'Act' being referenced	The full name of the Act has been included in the Joint Standard
Definitions and interpretation	Clarification on the definition of 'senior manager', IT asset, IT environment, IT infrastructure, software, supporting documentation.	Clarification on definitions were provided. The definitions for 'IT asset', 'IT environment' and 'IT systems' were slightly amended to create the relationships between the concepts. The definition for 'IT infrastructure' was removed from the Joint Standard as it was adequately catered for in the aforementioned concepts. The definition of 'software' was augmented to give examples and a definition of 'supporting documentation' was provided.
Application	Clarification on application to insurers vs insurance groups as well as the meaning of nature, scale and complexity.	The application section was amended to clarify that the Joint Standard applies to insurers as well as insurance groups. The application section was further augmented to indicate that the minimum requirements and principles must be implemented in consideration of the nature, size and complexity of the relevant financial institution.

Roles and responsibilities	Clarification on who is the 'governing body' and the alignment of the IT strategy with the business strategy (including for the need for separate strategy). There was also a request for specific requires relating where an independent role is being performed that the lines of defence or segregation of duties are maintained.	'Governing body' is defined in the FSR Act. The Joint Standard requires that the IT strategy, which may be aligned to the business strategy, is specifically identifiable. Where necessary, mention is made in the Joint Standard to the segregation of duties. The Authorities from a supervisory perspective will consider the segregation of duties as well as the lines of defence, where applicable.
IT strategy	Clarification was also sought on the point of notification for deviation from the IT strategy and possibility of contravention of financial sector laws.	The Joint Standard was amended to make it clearer when a notification is required.
IT risk management framework	Drafting suggestions on the inclusion of 'or make reference to policies and artefacts to the requirement of the composition of an IT risk management framework as not all aspects are covered within the IT risk management framework. Recommendation to expand the definition of 'IT Assets' to include IT Infrastructure and Physical security. Recommendation on the requirement to consider insurance as a risk mitigation factor being, that minimum service level and compliance requirements be set and aligned with Recovery and Resolution Planning requirements and the classification of information assets as per the POPIA and Information Regulator compliance requirements. Recommendation that this standard and insurance cover must also apply to critical financial service IT providers, not currently regulated. Making cybersecurity training available to all contractors and vendors with access to a financial institutions IT infrastructure and systems comes at a cost and is not practical in all cases	The Authorities disagreed with the suggestion as the policies, artefacts, standards etc that deal with managing IT Risk must be linked to the IT Risk Management Framework. Disagree with the recommendation. IT infrastructure and Physical Security cannot for the purposes of this Joint Standard be captured under IT Asset. Insurance is not the only measure to mitigate IT Risk. This Joint Standard applies to registered and licensed financial institutions. The financial institution remains responsible and accountable for IT risk despite it having outsourced certain functions or services. The financial institution must ensure when entering into contract with service providers that the financial institution is still able to comply with the requirements of this Joint Standard. The Joint Standard contains minimum requirements for IT Governance and Risk Management. Training of staff, service providers and contractors is a necessity and may be conducted in various cost-effective ways.
Oversight of IT Risk	Clarification sought on the definition of oversight in terms of the three lines of defence	Clarification was provided in the response.
IT Operations	Request for limiting the requirement to document IT operations by adding the words 'critical IT applications'. Drafting suggestion on the use of the word 'framework' instead of 'systems'. Recommendation to define 'criticality'. Clarification on the evidence required for capacity management.	The Authorities disagreed with the request as 'IT operations' encompasses more than just 'IT applications'. 'System' was removed and replaced with 'framework'. The Joint Standard does not define criticality and the classification of criticality is the prerogative of the financial institution. This classification will be considered, from a supervisory perspective, based on the nature, scale, complexity and risk profile of the financial institution. Clarification was provided on capacity management in the response.
Handling of sensitive and confidential information	Request for definitions of 'confidential', 'sensitive' as well as to include a requirement "to protect sensitive and confidential information such as customer personal account and personal information, including but not limited to the POPIA designated field and transaction data system".	The Authorities disagreed with the request as financial institution must comply with the POPIA legislation and it is not necessary for the Joint Standard to reiterate the requirements of POPIA. This Joint Standard does not define 'sensitive or confidential information' as this must be defined by the respective financial institution in consideration of other applicable legislation such as POPIA.
Risks associated with products and services	Drafting suggestion to include 'financial' before 'service and products'. The cost of capacity monitoring was raised.	'Financial' was included in appropriate references to products and services. The Authorities are of the view that the Joint Standard places minimum requirements on financial institutions in terms of IT Governance and Risk Management. Financial institutions must monitor utilisation to ensure that their systems are capable of handling loads.
IT programme and/or project management	Drafting suggestion to include the words 'policies' and 'standards' to the framework. Another drafting suggestion was to limit project plans to only material projects/programmes. Minor drafting suggestions were also proposed.	The paragraph was amended to reflect policies, procedures and processes as part of the framework. The determination of the materiality rests with the financial institution, the institutions decides if something warrants the establishment of a project or a programme. All projects and programmes related to IT must follow the governance processes and requirements stipulated in the Joint Standard. Minor drafting suggestions were accepted where deemed appropriate by the Authorities.
System recovery and business resumption	Drafting proposal to merge paragraphs. A request to reconsider the requirement for a disaster recovery (DR) site in consideration that an institution's strategy to manage DR could be the widespread use of cloud-based servers and off-site working, making a dedicated DR site unnecessary.	The drafting proposal was accepted. In terms of the DR site, the Authorities have amended the Joint Standard to cater for more than one DR site. The financial institution is required to demonstrate that they can recover services that are hosted in the cloud in the event that the cloud service provider is down. The paragraph requires a geographically separate DR Site which can mean that a financial institution that uses cloud services can access an alternate site provided by the cloud service provider if the provider's services are disrupted.
Assurance	Clarification on the definition of a 'control function' as well as the times for assurance.	A 'control function' is defined in the FSR Act. . The timelines depend on the IT assurance plan and the IT activities that have been conducted during a specific period. The Authorities will

		access the regularity based on the nature, scale and complexity of the financial institution as well as the IT activities that have taken place.
Notification and reporting requirements	Recommendation to include in the Joint Standard the notification parameters.	The Authorities will provide the parameters for notification in the form that will be determined.
General	Clarifications on exemptions from the requirements of the Joint Standard. Comment on the need for the Joint Standard to allow for sentiment towards the spirit of adherence/compliance as the delivery evidence of aspects of governance might not be available due to the rapid development of technologies. The Joint Standard should also not prohibit the flow and utilisation of technology advances and should not block efficiency with out of date or delayed governance requirements.	Section 281 of the FSR Act caters for exemptions. In terms of evidence of aspects of governance, these matters can be raised with supervisory team responsible for the financial institution and will be considered on a case-by-case basis. This Joint Standard is not meant to delay or hinder rapid changes. The financial institution is required to apply a risk-based approach but need to follow the necessary risk management and governance processes that should cater for rapid changes.

Table 5

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
1. Commencement				
1.	First Rand		No comment	Noted.
2.	BASA		No comment	Noted.
3.	Safire Insurance		No comment	Noted.
2. Legislative authority				
4.	First Rand		No comment	Noted.
5.	BASA	3.1	**Clarify** the Governing Body definition as it references Section 1 of the Act – which Act?	The 'Act' refers to the Financial Sector Regulation Act.
6.	Safire Insurance		No comment	Noted.
3. Definitions and interpretation				
7. .	First Rand	3.1	Consider including definitions for the terms 'cloud/cloud computing', 'outsourcing', and 'offshoring' as contained in the relevant directives of the PA because these terms are sometimes interpreted in different ways	The paragraphs dealing with 'outsourcing', 'cloud-computing' / 'cloud' and data 'offshoring' have been deleted from this Joint Standard and will be addressed through other regulatory instruments.
8.	FirstRand	Senior Management	The term 'senior management" in this standard contains some elements of the definition of "key person" in the Financial Sector Regulation Act but is not fully aligned. Is the intention for "senior management" to be considered as "key persons" under the FSR Act? If so, to ensure alignment to the enabling legislation, we recommend linking the definition to the FSR Act definition but contextualising which category of the FSR Act definition is relevant for this standard. Please note the above, implies throughout the standard.	Senior management does not include the board and control functions and the definition of key person includes the board and control functions. When reference is made to the senior management, it is within the context outlined above.
9.	BASA	3.1	**Clarify** the difference between IT Environment and IT Infrastructure. **Otherwise, recommend** that combine the two terms into one	IT environment is not limited to hardware and software. IT environment includes people, processes and the external environment. IT infrastructure is limited to hardware, software and its integrated components. The definitions have been amended to make the relationships clearer. IT infrastructure has been deleted from the Joint Standard.

10.	BASA	3.1	**Recommend** changing to material 'IT' Incident. **Recommend** adding 'system failure' to the definition as follows: *refers to a system failure, disruption of….*	It is not necessary to classify material 'IT' incident as a non-IT incident may affect IT systems. Refer to the requirement – where material incident is used – i.e. paragraph 15.1 – which reads that : A financial institution must notify the responsible authority of the financial sector law in terms of which the financial institution is licensed or registered, in the form and manner determined by the Authorities, **of any systems failure, malfunction, delay or other disruptive event**, within the determined timeframe after classifying the event as a **material incident**.
11.	BASA	3.1	independent review" – the definitions state that this may include internal and external audit, or an independent control function. Financial services are regulated according to the three lines of defence with the independent control functions being risk management and the independent assurance function being audit (internal or external). **Clarify** are functions such as compliance, business assurance and external specialists that report directly to the first line of defence also deemed independent control functions under this definition.	No. We are referring to the second line of defence any specialists etc. reporting to first line of defense is not considered to be independent. Control function is defined in the FSR Act as risk management, compliance function, internal audit and actuarial.
12.	Safire Insurance		No comment.	Noted.
13.	SAIA	Definition of 'software'	The current definition states that "'*software' means a set of programs and supporting documentation that enable and facilitate use of the computer*". This definition does not cover the various types of devices and the reference to "supporting documentation" is ambiguous. We recommend that this definition is expanded to include that "Software means a set of programs or applications that enable and facilitate the use of any computing device, such as a computer, server, mobile phone or tablet". We recommend that the Authorities explain the scope of "supporting documentation" in this context?	Noted. The paragraph has been augmented to include 'any computing devices such as computers or hand-held devices. In addition, a definition has been added for 'supporting documentation' - For the purposes of this definition – supporting documentation means all documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data.
			4. Application	
14.	First Rand	4.6	FirstRand recommends that we add "*and in conjunction with relevant financial sector directives and guidance notes from the Prudential Authority*" For example, directive D2-of-2019 on the reporting of material information technology and-or cyber incidents, amongst others.	Paragraph 4.6 by referring to 'financial sector laws' includes directives issues in terms of the Banks Act. We cannot include such specific details as this Joint Standard applies to financial institutions other than Banks.
15.	Safire insurance		No comment	Noted.
16.	SAIA	4.2 A financial institution that is a bank, or a controlling company must ensure that any potential risks relating to IT risk from juristic persons and branches structured under the bank or the controlling company, including all relevant subsidiaries approved in terms of section 52 of the Banks Act, 1990 (Act No. 94 of 1990), are catered for and mitigated in the application of the requirements of this Joint Standard.	The industry is not sure which definition would cover the non-life insurance in that, the Financial Institution is defined in accordance to the Banks act as per the standard We therefore request clarity on controlling company and financial institution for purposes of this Standard.	Paragraph 4.3 covers insurance groups and has been amended to refer to insurer and insurance groups.
17.	SAIA	4.5 The requirements of this Standard must be implemented in accordance with the nature, size, complexity, and risk profile of a financial institution.	We request clarity on what is meant by "*nature, size, complexity and risk profile of a financial institution"*	The Joint Standard contains minimum requirements. The requirements must be implemented in accordance with the nature, size, complexity and risk profile of a financial institution means that what is appropriate for a small financial institution will not be appropriate for a large financial institution.
			5. Roles and responsibility	
18.	First Rand	5.2	IT strategy cannot be separated from overall business strategy and it is considered unnecessary to have a separate, discrete strategy for IT. FirstRand suggests that this statement should be amended to "... *framework and must ensure that IT objectives are aligned and integrated with the organisation's strategy*	Please refer to paragraph 6.1 which states that - A financial institution must ensure that its IT strategy is approved by the governing body and aligned with its overall business strategy. Disagree with the comment as the Joint Standard is requiring an IT strategy.
19.	BASA	5.1	**Clarify** who the Governing body is and in which line of defence it resides. (CEO or Exco, The Board etc.)	The governing body is defined in the FSR Act. The Authorities hold the governing ultimately responsible for compliance with the requirements of the Joint Standard.

				Please note that this Standard also applies to institutions that may not have boards.
20.	BASA	General comment	**Recommend** that where there is an independent role being performed ensure that the lines of defence or segregation of duties are maintained or adhered to.	Noted. This will be considered from a supervisory perspective.
21.	Safire insurance		No comment.	Noted.
			6. IT Strategy	
22.	BASA	6.2	**Recommend** that the IT strategy of a financial institution must be reviewed regularly, at least annually, in the context of market, industry, technology and other **relevant** developments.	Noted, the Joint Standard has been amended accordingly.
23.	First Rand	6.3(a)	FirstRand's comments in section 5, No 3 has reference. FirstRand recommends removal of the words "…of its IT strategy." In the first sentence. Frequency of review of progress against IT objectives will vary amongst institutions; hence FirstRand recommends that the second sentence be amended to "…*reviewed regularly in accordance with the financial institutions internal processes to ensure relevance and appropriateness*".	Disagree. The Joint Standard requires an IT Strategy which can be aligned with the business strategy. The action plans review feed into the overall review of the strategy therefore the quarterly review is considered appropriate to track the progress in terms of the overall strategy review, which must be conducted at least on an annual basis. Please note that this was addressed in comment 152 of the Consultation Report.
24.	FirstRand	6.3(b)	FirstRand's comments in section 5, No 3 has reference. FirstRand recommends replacing the words "IT strategy" with "*IT objectives*".	Disagree. The Joint Standard requires an IT Strategy which can be aligned with the business strategy. Please note that this was addressed in the Consultation Report.
25.	FirstRand	6.I)	It is the FirstRand's view that this requirement may lead to a flood of reporting to the joint PA. Taking a risk based approached, it is FirstRand's recommendation that only material deviations from the IT strategy that may Clarity is also sought on the following: a) What is the purpose of the reporting? b) When must the deviation be reported i.e. before such deviation is considered by the Financial Institution (FI) or before implementation? c) Will reporting mitigate the risk of regulatory sanctions under this Standard and/or applicable financial sector laws? d) Will this report be kept confidential? It is our view that this type of information in the public domain may cause undue concerns and panic.	The deviation only relates to the potential that the Joint Standard may be contravened. It is not necessary to stipulate that it is material or not – the test is whether it will lead to a possible contravention of the Joint Standard or other legal requirements relating to IT risk. The form and manner for reporting will be consulted on prior to finalisation. (a) The purpose of the reporting is to advise the responsible authority of the potential risks and what actions have been put into place to ensure that the requirements of the Joint Standard are being met. (b) Noted, the paragraph has been amended to make the point of notification clear i.e., on discovery of the deviation and the possibility of contravention (c) Reporting is to inform the regulator and sanctions or mitigants will be considered when there is an actual contravention. (d) The Authorities comply with the provisions of section 251 of the FSR Act in this regard.
26.	BASA	6.3(c)	**Recommend** wording update: ensure that the appropriate Regulatory Authorities are informed when there is a material deviation.	Disagree. See response to comment 25 above.
27.	BASA	6.3(c)	Word "Legal": This is very broad. **Recommend** including the word *'material' deviation or legal requirement.*	Noted, the legal requirements have been limited to financial sector law and 'inform' was changed to 'notify'. In terms of the deviation, see response to comment 25 above.
28.	BASA		**Clarify** the rationale and practicality to be provided for – "ensure that the responsible authority for the financial sector law in terms of which the financial institution is licensed or registered is informed when there is a deviation from the IT strategy that may contravene this Standard or any other legal requirements relating to IT risk management."	See response to comment 25, 26 and 27 above.
29.	Safire Insurance		No comment.	Noted.
			7. IT risk management framework	
30.	First Rand	7.3(d)	Governing bodies may still have overall oversight or accountability, but consideration should be given to allowing for such delegations where reference is made to specific compliance obligations (apart from the governing body's obligation to have oversight and ultimate accountability	Please refer to comment 212 of the consultation report. Paragraph 5.3 defines the roles of the responsibilities of governing body. 7.3(d) does not preclude any delegations.
31.	FirstRand	7.3(e) (I) and (ii)	There exists no data structure/element in this assertion/prerequisite. While IT assets are traditionally viewed in terms of the hardware and software components, this has since evolved to consider more importantly the underlying data and its associated constructs/methods/structures and	Please refer to comment 226 of the consultation report. The Authorities have included a definition for information asset. The specificity of requirements is necessary for this Joint Standard.

			metadata. Specific mention around data and not simply “IT assets” is recommended. In addition, these statements are fairly detailed and specific, more appropriate for inclusion within an IT Asset Management Policy instead of an IT Risk Management Framework	
32.	FirstRand	**7.3(l) (iii)**	The Fit and Proper requirements in FAIS apply to FAIS appointed and approved representatives and Key individuals. It does not extend to all staff, vendors and contractors. The competency requirements set out in FAIS, apart from potentially the honesty, integrity and good standing, would not be relevant to all staff, vendors and contractors. BASA has made comments in the previous version of the draft standard to narrow the definition as qualifications may not always be relevant for all roles. The response document indicates that the regulators have now included the word “certification”. However when one reads the regulator response to similar and more detailed commentary, by Masthead for instance, it appears that sectoral laws, in this instance FAIS, may be seen to apply to staff, contractors and vendors who are not in FAIS roles – i.e. the response document refers to the application of sectoral laws (of which FAIS is one). Clarity is imperative on where the competency requirements related to this standard will be encapsulated and will there be prior consultation before those requirements are finalised. Will it there be reasonable transitional arrangements to meet those new requirements.	The FAIS legislation for fit and proper requirements will only apply to those persons that are captured in the FAIS requirement. This Joint Standard cannot extend the scope of the FAIS fit and proper requirements to include persons other than those capture under FAIS legislation. The Authorities have amended section 7.3(l)(iii) to limit the application to staff, vendors and contractors that are appointed for IT functions and services. This includes the requirement for being fit and purpose i.e., for the purposes of this Joint Standard, the fit and proper requirements are application to those staff, service, providers and contractors that are appointed for IT services and functions. To ensure consistency, ‘vendors’ has been changed to ‘service providers’.
33.	BASA	7.3	Word “Incorporate” **Recommend** adding the words *‘or make reference to the relevant policy or artefact’* as not all these aspects are included in the IT risk management framework but are included in other related bank policies/processes/standards	Disagree that the amendment is necessary. The policies, artefacts, standards etc that deal with managing IT Risk must be linked to the IT Risk Management Framework. The Authorities will as part of supervision consider how the risk management framework is structured.
34.	BASA	7.3	**Recommend** wording: *incorporated or linked to other policies, processes, and standards*	See response to comment 33 above.
35.	BASA	7.3(a) and (c)	**Recommend** merging (a) and (c) into one requirement: Must have policies, standards, and procedures to manage IT risks, which are independently reviewed and at least annually updated in line with rapid changes in the IT and security environment, by the relevant business area.	Disagree that the merging is necessary. The paragraphs adequate communicate the requirements.
36.	BASA	7.3 (c); 7.3 (d) iii	**Clarify,** was security not deliberately excluded from the scope of this document?	Information security has been excluded from the Joint Standard. In these paragraphs, the Authorities consider it necessary to include security.
37.	BASA	7.3 (e) (i)	IT Assets’ **Recommend** expanding on IT Assets to include IT Infrastructure and Physical security	Disagree with the recommendation. IT infrastructure and Physical Security cannot for the purposes of this Joint Standard be captured under IT Asset.
38.	BASA	7.3 (e) (ii)	**Recommend** that the definition of criticality be aligned with that of service and process criticality definition of Recovery and Resolution Planning requirements and the classification of information assets as per the POPIA and Information Regulator compliance requirements	The Joint Standard has not defined criticality. The classification of criticality is the prerogative of the financial institution. This classification will be considered from a supervisory perspective based on the nature, scale, complexity and risk profile. Information asset is defined for the purposes of this Joint Standard.
39.	BASA	7.3 (f) (ii)	The word “matrix” has been incorrectly included. **Recommend** wording change as follows: “*develop a method or process of assessing impact of the threats and vulnerabilities ~~matrix~~ to its IT environment ~~which should also~~ to assist the financial institution in prioritising IT risks*	Noted. The word ‘matrix’ has been deleted.
40.	BASA	7.3 (g) (iv)	The level and associated cost of insurance will be determined by the minimum service level, and legal and compliance requirements. IT services and infrastructure assets may also be outsourced to 3rd and 4th party service vendors onshore and or offshore. It will be difficult to enforce appropriate IT insurance coverage on critical financial service IT providers. **Recommend** that minimum service level and compliance requirements be set and aligned with Recovery and Resolution Planning requirements and the classification of information assets as per the POPIA and Information Regulator compliance requirements. **Recommend** that this standard and	Insurance is not the only measure to mitigate IT Risk. This Joint Standard applies to registered and licensed financial institutions. The financial institution remains responsible and accountable for IT risk despite it having outsourced certain functions or services. The financial institution must ensure when entering into contract with service providers that the financial institution is still able to comply with the requirements of this Joint Standard.

			insurance cover must also apply to critical financial service IT providers, not currently regulated	
41.	BASA	7.3 h(ii) i(i)	**Recommend** that the definition of criticality be aligned with that of service and process criticality definition of Recovery and Resolution Planning requirements and the classification of information assets as per the POPIA and Information Regulator definitions.	See response to comment 38 above.
42.	BASA	7.1	**Clarify** if this must be a Stand-alone IT Risk Management Framework or if can this form part of an Operational and Resilience Risk Framework. Considering each organisation has a different risk management approach and structure. **Recommend** wording: A financial institution must establish and or evidence an IT risk management framework to manage IT risks systematically and consistently.	Kindly refer to amendment made to paragraph 7.1 – where it is provided that the IT Risk Management framework may form part of an Enterprise Risk Management Framework. It is not a requirement to have a stand-alone framework. The financial institution must be able to demonstrate that the requirements of the Joint Standard are implemented within the structures of the financial institution.
43.	BASA	7.3 (b)	Recommend wording: the ability to identify, assess and manage all major and material risks, taking into consideration the principle of proportionality	Noted, 'major' has been changed to 'material'. .
44. .	SAfire Insurance	(d).(iv)	An individual with the requisite skills and experience, specifically in relation to cybersecurity risks, who is also a member of senior management is an expensive resource that is out of reach of many small to medium institutions. The Standard ought to allow for the flexibility to outsource such a function, with a member of senior management responsible for that outsourced function.	The standard does allow for the flexibility to outsource; however, the responsibility still lies with the regulated institution irrespective of whether the function is being outsourced.
45.	SAfire Insurance	(f)	The interpretation of 'threats', 'risks' and 'vulnerabilities' varies across the industry and is not defined in this standard. The Standard's definition of these elements would be necessary for financial institutions to clearly understand the level of detail required in the risk assessment prescribed in this Standard.	Please refer to comment 228 of the consultation report. With respect to the requirements of paragraph 7.3 (f), the Authorities will consider providing bilateral guidance on the matter on a case-by-case basis
46.	SAfire Insurance	(i).(iii)	Making cybersecurity training available to all contractors and vendors with access to a financial institutions IT infrastructure and systems comes at a cost and is not practical in all cases. As an example, contractors with access to IT infrastructure and systems may often be outsourced cybersecurity experts. A financial institution sending cybersecurity training to such a contractor would be redundant and wasteful. In addition, brokers and financial advisors, in their capacity as a vendor, will have access to multiple financial institutions' systems. This requirement makes it compulsory for all institutions to make training available to all vendors. This introduces a large amount of wasteful expenditure.	The Joint Standard contains minimum requirements for IT Governance and Risk Management. Training of staff, service providers and contractors is a necessity and may be conducted in various cost-effective ways.
47.	JSE	7.3(c)	Without the comma (after 'and') it implies that the independent review and the updates must be done by the relevant business area.	The independent review has been defined in the Joint Standard and cannot be conducted the business area. It must be conducted by independent party as outline in the Joint Standard. A comma after 'independent review' has been added.
48.	JSE	7.3(i)	(ii) develop a method of assessing **the** impact of the threat ~~and~~ against **the** vulnerability matrix ~~to~~ of its IT environment, which should also assist the financial institution in prioritising IT risks;	Note, the paragraph has been amended accordingly.
49.	SAIA	7.3(e)(ii)Criticality and sensitivity of IT assets must be identified and ascertained in order to develop appropriate plans to protect them.	We request clarity on the meaning of "*sensitivity*" in order to ensure common understanding	The Joint Standard has not defined sensitivity. The sensitivity of IT assets is the prerogative of the financial institution. This sensitivity will also be considered from a supervisory perspective based on the nature, scale, complexity and risk profile.
50.	SAIA	7.3(f) Identification and assessment of impact and likelihood of current and emerging threats, risks and vulnerabilities in terms of which a financial institution must	We require definition of "*threats, risks, and vulnerabilities*" in order to ensure common understanding.	The Authorities are not prescriptive on the format and minimum content of the threat and vulnerability matrix, as it is performed based on nature, size and complexity of the institution. However, the Authorities will consider providing bilateral guidance on the matter on a case-by-case basis.
51.	SAIA	7.3(i)(i) The financial institution must ensure careful screening and selection of staff, vendors and contractors in order to minimise IT risks due to system failure, internal sabotage or fraud;	We require that contractors be defined as for purposes of this Standard taking into consideration that insurers deal with different types of contractors. Furthermore, what specific screening would be required by the Authorities in order to meet the Standard?	Please refer to comment 32 above. The Authorities are not prescriptive on the type of screenings conducted. The financial institution must be satisfied that the contractors, staff, service providers appointed for IT services or functions are fit and proper.
52.	SAIA	7.3(i)(ii)(aa) Fit and proper	We require clarity on who will manage/oversee the fit and proper process?	The Authorities are not prescriptive on who manages and outsees the fit and proper processes. Financial institutions must follow their policies, processes and procedures in appointment of fit and proper persons. The Authorities will hold the governing board ultimately responsible for compliance with this Joint Standard.

			8. Oversight of IT risk management	
53.	First Rand	8	Regulation needs to be balanced between principles and rules. We suggest that the reporting line structure is informed by the organisational roles and responsibilities as specified by mandated senior executives outside of the governing body. With regard to the reference to "direct reporting lines to the governing body": we suggest that the reporting line structure should be informed by the organisational roles and responsibilities as specified by mandated senior executives, who may potentially have reporting lines outside of the governing body	Please refer to comment 263 of the consultation report. The word 'direct' has been removed.
54.	BASA	General	**Clarify** the definition of oversight in terms of the three lines of defence risk management regulations.	Oversight: first-line will be management oversight; then second-line will be compliance and risk management; then internal audit will be the third-line.,
55.	SAfire Insurance		No comment.	Noted.
			9. IT operations	
56.	First Rand	9.3(a)	a) Documenting of critical IT operations – can this be reworded to maintaining a register of critical IT applications?	The Authorities are of the view that this might be limited to only IT applications. The IT operations encompass all aspects.
57.	FirstRand	9.3 (g) +9.3(h)	There are elements of duplication here and in 9.2 e.g. requirement for incident and change process.	Paragraph 9.2 primarily refers to governance structure while 9.3(g)+9(h) refers to process of change, incident and problem management.
58.	BASA	9.1 and 9.2	IT service management policies, standards, processes, and procedures make up an IT service management framework – the previous term was more appropriate than the change to "system". **Recommend** keeping it as a "framework". **Recommend** differentiation between the methodology and practice (i.e., framework) vs. the technical tools used for service management (e.g., incident and ticket logging system).	Noted. 'System' has been removed. 'Framework' has been added in brackets. ' Paragraph 9.2 was also changed from 'system' to 'Framework'.
59.	BASA	9.3(a)	**Recommend** that the definition of criticality be aligned with that of service and process criticality definition of Recovery and Resolution Planning requirements and the classification of information assets as per the POPIA and Information Regulator compliance requirements.	The Joint Standard has not defined criticality. The classification of criticality is the prerogative of the financial institution. This classification will be considered from a supervisory perspective based on the nature, scale, complexity and risk profile of the financial institution. Information asset is defined for the purposes of this Joint Standard.
60.	BASA	9.3(d)	This will be extremely cumbersome without clear tangible benefits. **Recommend** that this only be applied to IT assets that support services and processes defined as critical by Recovery and Resolution Planning requirements, the classification of information assets as per the POPIA, Information Regulator compliance requirements or as per other mandatory compliance requirements	The Authorities are of the view that this requirement is essential to ensure proper IT governance and risk management.
61.	BASA	9.2	**Clarify** Capacity Management and if it is related to infrastructure or resource/staff as part of people risk. **Recommend** providing wording to allow for the case where capacity management evidence might be limited or not possible to capture.	It refers to the infrastructure.
62.	BASA	9.2(e)	Define the evidence for capacity management. Increased costs and management oversight may be counter-productive and excessive.	The capacity management refers to network bandwidth, mail servers, servers, data storage.
63. .	SAfire Insurance		No comment	Noted.
			10. Handling of sensitive and confidential information	
64.	FirstRand	10.1(a)	FirstRand suggest that this statement be amended to "*protect sensitive and confidential information such as customer personal account and personal information, including but not limited to the POPIA designated fields and transaction data in systems*;" "sensitive or confidential information" definition must be aligned with the definitions of Personal Information and Special Personal Information in POPIA. It is also important that the use of the word "confidential" is defined if used here, as it's applicability is wider than "privacy".	Disagree, the financial institution must comply with the POPIA legislation, and it is not necessary for this Joint Standard to reiterate the requirements of POPIA. This Joint Standard does not define 'sensitive or confidential information' as this must be defined by the respective financial institution in consideration of other applicable legislation such as POPIA. The amended Joint Standard does not refer to 'privacy'.

			A reading of the draft clause 11.2 (e) suggests that the words 'sensitive or confidential information" is being used synonymously with the POPIA definitions. Suggestion that this be aligned across this Standard and POPIA. FirstRand notes that information risk is a separate risk type and not part of IT or technology risk. This is a critical distinction as the objectives, accountability, resourcing and governance of information risk is entirely separate from IT/technology risk. FirstRand suggests that consideration be given to removing this from the IT/technology risk standard and addressing it separately. This point is reflected within King IV as well.	In paragraph 10.1(a), the Authorities are merely providing examples in the context of the business of the financial institution in relation to sensitive or confidential information. This standard is concerned with information that is not paper based but is intrinsically linked to the IT system. The Joint Standard has been amended to exclude paper-based information in the definition of information asset. This section of the Joint Standard captures requirements in relation to information in so far as it creates an IT risk and risk to customers.
65. .	BASA	10	**Recommend** that this should be covered under an Information Risk Management standard or policy	Refer to response to comment 64 above.
66. .	SAfire Insurance		No comment.	Noted.
10. Risks associated with products and services				
67.	First Rand	11.2(d)	This Draft Standard correctly recognises the FSR Act as the "legislative authority" and notes that "In this Standard, 'the Act' means the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) and any word or expression to which a meaning has been assigned in the Act bears the meaning so assigned to it, and unless the context indicates otherwise". The FSR Act refers to a "financial product" or a "financial service". We suggest that all references in this Draft Standard to "product(s) or service(s)" should be replaced with "financial product(s) or financial service(s)".	Noted. Where deemed appropriate this has been amended.
68.	BASA	11.2(e)	Cost of capacity monitoring may in some cases not be possible. **Recommend** that the wording be updated to "where possible implement measures to plan and track capacity utilisation as well as guard against online attacks".	This Joint Standard place minimum requirements on financial institutions in terms of IT Governance and Risk Management. Financial institutions must monitor utilisation to ensure that their systems are capable of handling loads.
69. .	SAfire Insurance		No comment	Noted.
11. IT Programme and/or project management				
70. .	First Rand	12.2(a)	The standard mentions "A financial institution must develop a framework". FIs may have the requirements defined in any of a framework, policy or standard for project management. FirstRand suggests that the statement be amended to cover any of these by rewording to "A financial institution must develop a framework or policy or standard and approach…". In addition, FirstRand is of the view that not all projects are material and important enough to have such a detailed plan, and hence suggest that the statement be amended to clarify that these requirements be limited to those projects/programmes which are deemed by the FI to be material/significant.	The framework may be incorporated in other documents provided that it is clearly identifiable. The paragraph was amended to reflect policies, procedures and processes as part of the framework. The determination of the materiality rests with the financial institution, the institutions decides if something warrants the establishment of a project or a programme. All projects and programmes related to IT must follow the governance processes and requirements stipulated in the Joint Standard.
71.	FirsRand	12.2(f)	The standard only references the risk of unverified changes in this section. There are other risks which are mitigated through having a mirrored pre-prod environment segregated from Production etc. FirstRand therefore suggests the removal of this reference from the statement.	Noted. The paragraph has been amended by deleting 'unverified changes' and replacing it with 'risks introduced'.
72. .	BASA	12.1	**Recommend** wording: *framework or policy*	See response to comment 70 above.
73.	BASA	12.2 (K)	**Recommend** a point for risk management involvement and independent risk assessment.	IT assurance as provided for in paragraph 14 of the Joint Standard covers this point.
74. .	SAfire Insurance		No comment	Noted.
75.	JSE	12(1) 12.2 12.2 (b)	Add 'its' before IT programme Delete ''s' from that includes (b) ensure that its IT programme and project management polic**ies, procedures and processes**~~y~~ confirm~~s~~ that IT security requirements are	Noted, amendments have been made accordingly.

			analysed and approved by a function that is independent from the development function;	
12. System Recovery and business resumption/IT resilience and business continuity				
76. .	BASA	13.10	This is duplicated/overlapping with paragraph 13.4. The only difference is the wording “returning to a state of normality” which seems to refer to the same requirement of re-establishing the confidentiality, integrity, and availability of business functions as per 13.4. **Recommend** removing 13.10 or merging with 13.4.	Noted. Paragraph 13.10 has been merged with Paragraph 13.4.
77. .	SAfire Insurance	(b)	This requirement alludes to a single DR site where key staff can operate from should the institution be affected by a disruptive event to their primary site. In the age of working home and cloud services, this is an unnecessary requirement. An institution’s strategy for managing DR could be the widespread use of cloud-based servers and off-site working, making a dedicated DR site unnecessary.	Noted. The paragraph has been amended to cater for more than one disaster recovery site. The financial institution is required to demonstrate that they can recover services that are hosted in the cloud in the event that the cloud service provider is down. The paragraph requires a geographically separate DR Site which can mean that a financial institution that uses cloud services can access an alternate site provided by the cloud service provider if the provider’s services are disrupted.
78. .	First Rand		No comment.	Noted.
79. .	SAfire Insurance		No comment	Noted.
80.	SAIA	13.1(a) define system recovery and business resumption priorities and establish specific Service Level Objectives including RTOs and RPOs for critical services and business processes;	The statement does not take into account cloud services or work from home environment. It uncompromisingly requires the insurer to establish disaster recovery sites as geographically separate. Is it necessary to have a separate DR site with cloud-based services in place?	See response to comment 77 above.
81.	SAIA	13.(1)(b) identify and establish a disaster recovery site that is geographically separate from the primary site to enable the recovery of critical systems and continuation of business operation disruption occur at the primary site ns, should a	The work environment and technological developments have introduced cloud service and work from home functionalities. As a result, physical servers have become redundant, and the DR may subsequently follow suite. We require the Authorities to consider the probability of the geographical requirement of the DR becoming redundant.	See response to comment 77 above.
82.	JSE	13(2)	13.2 A financial institution must conduct a business impact assessment by analysing its exposure to severe business disruptions and assessing its potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (for example a third-party provider **of** data relevant to a business process or publicly available data that may be relevant to the business impact assessment) and scenario analysis.	Noted, the amendment has been made accordingly.
83.	SAIA	13.12 A financial institution must test the recovery dependencies between systems. Bilateral or multilateral recovery testing must be conducted where networks and systems are linked to specific service providers and vendors, where applicable. If bilateral or multilateral recovery testing is not possible due to significant risks, the responsible authority for the financial sector law in terms of which the financial institution is licensed or registered, must be notified	Certain parts cannot be tested based on third-party users, as a result the standards may be impractical. What is the intention of this paragraph? Could it be that the Authorities may have to consider the change in environment and amend the Standard accordingly? We require clarity in respect of the following: - • Will there be a “form” for the notification? • Who will need to be notified; and • What will be the timelines?	The intention of the paragraph is that financial institution must test recoverability and dependency between systems. The responsible authority in terms of which the financial institution is licensed or registered must be notified. The paragraph has been amended to add that: The notification must be done in the form, manner and time-period determined by the Authorities.
13. Outsourcing (Removed from the Joint Standard)				
84. .	BASA	14	While G5/2014 covers much of this, outsourcing is expected to be dealt with in a separate Joint Standard. **Recommend** that some references be included even if at a high level regarding a need to identify, assess, and manage third-party risks (i.e., broader than just outsourcing) relating to technology providers. This should include inter alia appropriate due diligence, scrutiny of third-party control, ongoing oversight, and assessment of potential concentration risk (internal and/or systemic).	This has been done through specific requirements e.g., in paragraphs 13.2, 13.3, 13.6, 13.12 and 7. This must also be considered in terms of general risk management principles.

85. .	SAfire Insurance		No comment	Noted.
14. Assurance				
86. .	First Rand	14.1	Reference is made in this section to an “control function” but there is no definition for this. FirstRand requests clarity on which function is being referred to here as not all organisations would have such a function. Once clarity is provided, FirstRand would like the opportunity to provide a response to this section.	Control function is defined in the FSR Act. The requirements relate to a control function or an external assurance provider. The consultation period for the Joint Standard has closed.
87.	SAIA	14.1 The control functions and/or external assurance providers, must have the capacity to independently review and provide objective assurance of compliance with all IT -related activities as outlined in the financial institution’s policies and procedures as well as with external requirements	We require clarity on the following: - • What are the timelines on this, annually, bi-annually? • May it be done externally?	Yes, it can be done externally through an external assurance provider. The timelines depend on the IT assurance plan and the IT activities that have been conducted during a specific period. The Authorities will access the regularity based on the nature, scale and complexity of the financial institution as well as the IT activities that have taken place.
88.	BASA	14(c)	**Recommend** for inclusion: Overall IT Assurance Plan should be inclusive of the Three Lines of Defence.	It was removed as some financial institutions do not have the three lines of defence. However, the requirement refers to control functions and the assurance can be provided through the second and third lines of defence.
89.	SAfire Insurance		No comment	Noted.
15. Reporting/Notifications and reporting requirements				
90. .	BASA	15.2	**Recommend** wording: *The Regulatory Authorities*	Disagree, Authorities has been defined.
91.	BASA	15.1	**Recommend** inserting the SLA for notification to the regulator should there be a Material incident (Severity 1 or Severity 2 Incident). **Clarify** the lines of communication is acceptable, the process to be followed, the root cause analysis requirements and the lessons learnt assessment to close out the notification. This will help there to be consistency across the financial sector.	These will be provided for in the forms that will be determined by the Authorities.
92.	SAfire Insurance		No comment	Noted.
93.	First Rand		No comment.	Noted.
2. GENERAL COMMENTS				
94. .	First Rand	General	The minimum requirements are very detailed, will there be an exceptions process in cases where an FI is unable to meet the minimum requirements as all requirements will not be achievable all the time? If there is to be such a process, then FirstRand recommends that only material deviations be reportable.	The FSR Act does provide for exemptions in terms of section 281 as well as extension of period of compliance in terms of section 279. These will be considered on a case-by-case basis.
95. .	BASA	General	The standard needs to allow sentiment towards the spirit of adherence/compliance. Within the rapid development of technologies and development, the delivery evidence of aspects of governance might not be available, however, it does not mean the organisation does not show a willingness to comply.	These matters can be raised with supervisory team responsible for the financial institution and will be considered on a case-by-case basis.
96.	BASA	General	The general theme of the standard should not prohibit the flow and utilisation of technology advances. When referring to rapid development and automated change deployment (with due governance) the standard should not block efficiency with out-of-date or delayed governance requirements that prohibit advancements and time-to-market delivery.	This Joint Standard is not meant to delay or hinder rapid changes. The financial institution is required to apply a risk-based approach but need to follow the necessary risk management and governance processes that should cater for rapid changes.
97. .	SAfire Insurance		No comment	Noted.
98. .	General Reinsurance Africa Limited	Section 10 Section 15 Section 17	Section 10, section 15 and section 17 (24-hour notification window was abandoned) have been removed. This means that the concerns we raised in the previous round of comments were addressed.	Noted. The time period within which to notify the Authorities will be determined in the form.

99.	General Reinsurance Africa Limited		There is a great deal of emphasis on resilience now, which agrees with our IT security strategy.	Noted.
100	SAIA		The proposed implementation conflicts with the Regulatory Plan, please confirm the correctness therein. Confirm exact dates for implementation transitional period	It is envisaged that the Joint Standard will become effective in 2024 but will being published in 2023.