SOUTH AFRICAN RESERVE BANK
Prudential Authority

Joint Standard: Cybersecurity and cyber resilience requirements

Consultation Report

June 2023

Contents page

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: Cybersecurity and Cyber Resilience Requirements.**

2. Summary of the consultation process

2.1 On 15 December 2021, the Financial Sector Conduct Authority and Prudential Authority (hereafter jointly referred to as "the Authorities") published the following documents in terms of section 101 of the FSR Act for the first public comments, with the comments due on 15 February 2022:

(a) the draft Joint Standard;
(b) the draft statement of need for, expected impact, and intended operation of the draft Joint Standard (Statement); and
(c) the comments template providing the manner in which comments must be submitted to the Authorities as well as questions.

2.2 On 14 December 2022 the Authorities published the following documents for the consultation in terms of section 98 of the FSR Act, with comments due on 28 February 2023:

(a) the revised Joint Standard based on comments received from the 2021 public consultation process;
(b) the Statement;
(c) the comment matrix from the 2021 public consultation process;
(d) the draft notification template; and
(e) the comment template.

2.3 The Authorities received over 300 comments from 36 respondents following the 2021 public consultation process. Where appropriate, certain comments resulted in amendments being made to the Joint Standard by the Authorities. Subsequent to the 2021 consultation, the second public consultation process conducted in 2022 resulted in over 250 comments being received from 23 respondents.

2.4 A general account of issues raised during the consultation process and the response of the Authorities, details of the commentators from the 2022 public comments, as well as the full set of comments are attached hereto as Tables 1, 2, and 3 below.

2.5 A general account of issues raised during the consultation process and the response of the Authorities, details of the commentators from the 2021 public comments, as well as the full set out comments are attached hereto as Tables 4, 5, and 6 below.

Table 1 – Summary of the comments received during the 2022/2023 consultation

No.	Paragraph of the Joint Standard	Summary of comments	Response from the Authorities
1.	Commencement of the Joint Standard	• Institutions were concerned about the transitional period and indicated that we need to consider giving sometime to enable them to perform a detailed gap analysis of existing controls against the proposed Joint Standard. • Smaller entities may also struggle to meet the compliance deadlines for the Joint Standard.	• It is the view of the Authorities that a 12-month transitional period is adequate for preparation to ensure full compliance with this Joint Standard. • The Joint Standard will be published and from the publication date a 12-month period will be given to financial institutions to implement the requirements of the Joint Standard. • Extensions for compliance will also be considered on a case-by-case basis.
2.	Definitions and interpretation	• Request for clarity on certain terms used in the Joint Standard as well as recommendations on specific terms. New definitions were also proposed.	• Clarification was provided on terms already defined. Additional terms were also defined such as cryptography, privilege account and privilege users. Definitions were also expanded on or streamlined in terms of the comments received.
3.	Roles and responsibilities	• Clarity is sought as to whether the delegation to senior management committees is acceptable alternatively whether the standard is referring to Board Committees such as Audit and Risk Committee? • Clarity is sought as to whether this covers all third parties or specifically to Information Technology third parties. We would recommend that the timeframe to comply be extended to 24 months as challenges may be experienced in covering all third parties within 12 months due to the utilization of various systems across third parties.	• The board is ultimately responsible and accountable for compliance with the Joint Standard to the Authorities. Delegation may occur as the board deems fit. • The Joint Standard covers all third parties that have access to the institution's information assets, however, institutions can apply for extension to comply in terms of section 279 of the FSR Act.
4	Governance	• Clarity is sought as to whether the standard is requiring structural changes to the reporting lines of the CIO directly into the Governing Body and the information security functions reporting line away from the Chief Information Officer.	• The Standard is requiring additional reporting lines. Paragraph 6.1.4 has been amended to include control functions.

Table 1 – Summary of the comments received during the 2022/2023 consultation

No.	Paragraph of the Joint Standard	Summary of comments	Response from the Authorities
5.	Cybersecurity strategy and framework	• Clarification on whether the cybersecurity strategy and framework must be separate documents or whether it can be combined with existing documentation. • Clarity on accountability of firms to which roles have been outsourced. • Clarity on reviewing of frameworks regularly vs annually • The practicality to perform an independent review of the adequacy and effectiveness of the cyber security framework annually – propose 3 year reviews rather	• Where an institution has an enterprise risk management framework, it may incorporate the requirements into the framework provided that its incorporation is demonstrable to the Authorities. • It remains the ultimate responsibility of the financial institution. The contract is between the financial institution and the third party and the provisions relating to recourse should be specified in the contract. • Regularly vs annually depends on the nature, size, complexity of the financial institution. • The Authorities do not support a 3-year review. Refer to the definition of independent review in the Joint Standard. The review can be conducted by an internal or external audit function or an independent control function.
6		• Clarification on remote access requirements in the Joint Standard. • Difficulties in requiring third-party providers to have equivalent security • Encryption of all sensitive data • Application of the requirement for cloud computing and storage. • Requirements for vulnerability assessment to smaller financial institutions.	• Each device that should access your network should be configured with the minimum-security standards of the financial institution. • The Authorities are of the view that this is a critical requirement to safeguard financial institutions. Kindly refer to the Statement of need for and the expected impact. • In terms of encryption the authorities have retained the power to require encryption based on the nature, scale, complexity and risk profile of a financial institution. • A Directive and Guidance Note have been issued to Banks on cloud computing. The Authorities will in due course publish, for consultation, a Joint Standard on cloud computing which will apply to the insurance sector as well. However, the principles and requirements captured in this standard in so far as cybersecurity and cyber resilience will

Table 1 – Summary of the comments received during the 2022/2023 consultation

No.	Paragraph of the Joint Standard	Summary of comments	Response from the Authorities
			apply to relationships with third-party service providers, including cloud computing service providers. • The Joint Standard, provides proportional implementation of the relevant requirement and same must be assessed in consideration of the nature, size, complexity and risk profile of a financial institution. In this light, an appropriate "vulnerability assessment" and "penetration testing" must be applied, taking into account the size and nature of the financial institution. In addition, when implementing and assessing these requirements, the Authorities will apply supervisory discretion and possibly light touch regulation, taking into account the type, size, nature and complexity of a financial institution.
7.	Cybersecurity hygiene practices	• Applicability of multi-factor authentication • It is not always practical in all instances for security patches to be tested prior to it being applied to the IT system.	• Applies in cases where financial institutions have identified critical systems – which varies from financial institution to financial institution. • The Authorities are of the view that it would be difficult to ensure adequate compensating controls if the financial institution has not tested the security patches and understood its impact on systems and the IT environment.

Table 2 – Details of commentators - consultation 2022/2023

#	Commentator	Contact person	Acronym
1	**Association of Savings and Investments South Africa**	Johann van Tonder, Senior Policy Advisor	**ASISA**
2	**Assupol**	Solly Keetse	**Assupol**
3	**Aurora Insurance Company Limited**	Angelique Botha	**Aurora Insurance**
4	**Banking Association South Africa**	Mcdonald Madeyi, Prudential Manager	**BASA**
5	**Batseta Council of Retirement Funds for South Africa**	Anne-Marie D'Alton	**Batseta**
6	**BrightRock**	Frikkie Pretorius	**Brightrock**
7	**Brolink (Pty) Ltd**	Christoph Fuhrmann, Executive Head of IT	**Brolink**
8	**ENS Africa**	Jessica Blumenthal, director	**ENS**
9	**Financial Intermediaries Association**	Samantha Williams	**FIA**
10	**FirstRand**	Jace Mudali	**Firstand**
11	**Grindrod Bank**	Prishani Kasaven	**Grindrod**
12	**Guardrisk**	Jessica Kutumela, Chief Risk Officer	**Guardrisk**
13	**JSE Clear (Pty) Ltd**	Anne Clayton, Head: Public Policy & Regulatory Affairs	**JSE Clear**
14	**JSE Ltd**	Anne Clayton, Head: Public Policy & Regulatory Affairs	**JSE Ltd**
15	**Marsh (Pty) Ltd**	Michael Davies	**Marsh**
16	**Momentum Metropolitan Limited**	Nico Kotze, Head of Information Security Craig Summers, Head GRIT risk Verily Buso, Group Head of IT Risk	**MMI**

17	**Moody's**	Liam Gibbon, VP Government, Public and Regulatory Affairs	**Moody's**
18	**Netcash**		**Netcash**
19	**OUTsurance Insurance Company Limited, OUTsurance Life Insurance Company Limited and OUTsurance Holdings Limited**	Maretha Hurter, Head of Compliance	**OUTsurance**
20	**South African Insurance Association**	Themba Palagangwe	**SAIA**
21	**Standard Bank**	Winston Seyama Lisa Pienaar De Gouveia	
22	**The South African Institute of Stockbrokers**	Erica Bruce, SAIS President Kashnie Naidoo, Technical Consultant	**SAIS**
23	**Willis Towers Watson**	Dr Erich Potgieter, Associate	**WTW**

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
1.	Marsh	Cover page: Objectives and Key requirements	Second sentence: " *It is the responsibility of the governing body of a financial institution to ensure that the financial institution meets the requirements set out in this Joint Standard on a continuous basis."* It would be prudent to provide a guiding /recommended time frame as this current statement could be understood and interpreted differently.	Continuous means that there should be non-stop compliance with the requirements of the Joint Standard.
2.	Aurora Insurance	1.Commencement	Duly noted.	Noted.
3.	BASA	1. Commencement 1.1 This Joint Standard commences on Day-Month-2023	We have noted feedback from the authorities on page 5 of the comments Table, which provides that a 12-month transitional period will be provided, per the extract below and are comfortable with same.	Noted.
4.	Brightrock	1.1 Commencement Date	This standard has major implications for the way most organisations currently operate, and it will take some time to prepare for the new requirements the standard introduces. It is suggested that the Joint Standard commences on the 1st of December 2023 to give organisations sufficient time to adapt and transition to the new requirements.	Noted.
5.	FirstRand	1. Commencement 1.1 This Joint Standard commences on Day-Month-2023	We have noted feedback from the authorities on page 5 of the comments Table, which provides that a 12 month transitional period will be provided, per the extract below and are comfortable with same: "…It is the view of the Authorities that a 12-month transitional period is adequate for preparation to ensure full compliance with this Joint Standard. The Joint Standard will be published and from the publication date a 12-month period will be given to financial institutions to implement the requirements of the Joint Standard…the Authorities are of the view that the 12-month period will provide sufficient time for readiness.	Noted.
6.	FIA	1	- A 12-month implementation strategy is not sufficient for the implementation of a comprehensive Cyber Security Strategy that would meet the compliance requirements of	The comment is noted. Based on the criticality of the risk involved, the Authorities are of the view that the 12-month period is sufficient. Should the

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			the Revised Joint Standard – Cybersecurity and Cyber Resilience - These strategies are usually set over a 2 – 5-year period due the complexity, financial impact, recruitment of persons with the required skill sets, with an annual review to ensure goals are being met and executing remedial action if required. - References: o State of Illinois Cybersecurity Strategy: https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Pages/cybersecurity.aspx o U. S Department of Energy: https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf	smaller financial institutions require more time for compliance an application should be sent to the Authorities with motivations and set timelines for compliance.
7.	Marsh	Section 1: Commencement	It is recommended that the 12 month transition period is explicitly noted in this section.	The commencement date which will be 12 months from the publication date will be reflected in the table under this section.
8.	MMI	Commencement	We urge the joint regulators to consider a transitional period of greater than 12 months after the commencement of the joint standard. The joint standard remains onerous and will likely require more than 12 months to fully implement considering all other competing responsibilities. Furthermore, we request a stabilisation period of at least three months post - implementation to ensure implementation was successful.	See response to comment 6 above.
9.	Marsh	Section 2: Legislative Authority	No comment.	Noted.
10.	Aurora Insurance	2.Legislative authority	Duly noted.	Noted.
11.	Aurora Insurance	3. Definitions and interpretation	Duly noted. We have already incorporated and aligned these definitions into our existing Cybersecurity framework. It	Noted.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			appears that certain definitions have been shortened in this draft. We've retained the longer versions where appropriate.	
12.	ASISA	3. 'cyber incident'	It is proposed to insert the word *"retrieved*" after *"stored"* to cover all possible computerised actions and to align with the definition of "data" to read as follows: 'cyber incident' means a cyber event that – (a) jeopardises the cybersecurity of an IT system or the information processed, stored, **retrieved** or transmitted by the system; or	Noted. The word retrieved has been added to the definition of cyber incident.
13.	ASISA	3. 'data'	It is proposed to insert the word ***"processed"*** before *"stored"* to cover all possible computerised actions and to align with the definition of "cyber incident" to read as follows: 'data' means a subset of information in an electronic format that allows it to be **processed,** stored, retrieved or transmitted;	We have aligned the definition of data to the Electronic Communications and Transactions Act.
14.	ASISA	3.'sensitive information'	The word *"persons"* include both natural and juristic persons and would therefore also include juristic persons that are not financial institutions. It is proposed to replace the word "*individuals"* with ***"persons"*** to read as follows: 'sensitive information' means information or data where loss, misuse, or unauthorised access to or modification of could adversely affect the public interest of a financial institution or the privacy to which ~~individuals~~ **persons** are entitled;	Noted. The Joint Standard has been amended accordingly.
15.	ASISA	'3. vulnerability assessment'	The current definition of "*vulnerability assessment*" is inconsistent with the generally accepted definition and may be confused with a "*risk assessment*". A "*risk assessment*" includes "*a systematic review of controls and processes*". A	Disagree. The definition of 'vulnerability assessment' in the Joint Standard is adapted from the NIST definition and only defers on the reference to IT system, controls and

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			"*vulnerability assessment*" usually looks for vulnerabilities in a system. It is proposed to use the NIST definition: ***"Systematic examination of an information system or technology product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation."***	process vs information system in the NIST definition.
16.	Guardrisk	Vulnerability Assessments	The current definition of "vulnerability assessment" is inconsistent with the generally accepted definition and may be confused with a "risk assessment". This is because a "risk assessment" includes "a systematic review of controls and processes", this is not done in a vulnerability assessment, which usually just looks for vulnerabilities in a system. We would recommend using the NIST definition: " Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation."	See response to comment 15 above.
17.	FirstRand	3. Definitions and interpretation **cyber'1** means relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data and IT systems;	We recommend that this definition specify internet interconnected systems, because our internal network may not fall into the definition of cyber.	The Authorities are of the view that limiting this definition will result in major gaps and weaknesses in the risk that is being mitigated.
18.	BASA	3. Definitions and interpretation	We recommend that this definition specify internet interconnected systems, because our internal network may not fall into the definition of cyber.	See response to comment to 17 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		cyber'1 means relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data and IT systems;		
19.	FirstRand	3. Definitions and interpretation '**data**' means a subset of information in an electronic format that allows it to be stored, retrieved or transmitted;	Consider aligning the definition of data in the standard with the definition of data in ECTA - "data" means electronic representations of information in any form. Especially considering ECTA is the legislation that gives legal recognition to data and electronic messages.	Noted and amended accordingly.
20.	BASA	3. Definitions and interpretation 'data' means a subset of information in an electronic format that allows it to be stored, retrieved or transmitted;	Consider aligning the definition of data in the standard with the definition of data in ECTA - "data" means electronic representations of information in any form. Especially considering ECTA is the legislation that gives legal recognition to data and electronic messages.	See response to comment 19 above.
21.	FirstRand	3. Definitions and interpretation	• There is currently no definition for "Governing Body" on the Joint Standard. We understand as per the comments the FSCA has indicated that the definition of "Governing Body" is provided in the Financial Sector Regulation Act, 2017. This should still be inserted on the Joint Standard for ease of reference as the FSCA has done for the definition of '**investment fund administration services' means intermediary services referred to in paragraph (b)(i) of the definition of "intermediary service" as defined in the Financial Advisory and Intermediary Services Act,**	Disagree. As mentioned previously, "governing body is defined in the Financial Sector Regulation Act and clause 1 states that terms defined in the Financial Sector Regulation Act has that same meaning in the Standard. The example provided is not comparable because the term cited

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			2002 (Act No. 37 of 2002), performed in relation to a collective investment scheme or hedge fund. Therefore, the definition in the Joint Standard of "Governing Body" means "governing body as defined in the Financial Sector Regulation Act, 2017." The application of the Joint Standard does not include brokerages or CAT 1 FSP's other than a CAT 1 FSP that provides "investment fund administration services" as part of the definition of "financial institution". The definition does however refer to Insurers. Would this mean that insurers through delegation ensure that brokerages have an adequate cyber risk and cyber resilience policy?	(investment fund administration services) is not defined in the Financial Sector Regulation Act. .. The Standard does not at this stage apply to brokers for the reasons explained in the Statement of Need. The Standard also does not impose an obligation on an insurer to ensure brokers have an adequate cyber risk and cyber resilience policy. An insurer has to comply with the Standard and to the extent that it applies to the insurer. With regards to the application of this Joint Standard to CAT I FSP's, please note that the Standard applies to the financial institutions as defined. Therefore, the insurer is ultimately responsible for complying with the requirements in the Standard. Notwithstanding the above, it is incumbent upon the insurer to ensure that the third parties it engages with or outsource

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
				certain functions, have the requisite operational ability. Lastly, the FSCA as part of its Harmonization and Transition Projects, will develop a cross cutting Standard that will apply to other financial institutions not contemplated in the Joint Standard.
22.	BASA	3. Definitions and interpretation	There is currently no definition for "Governing Body" on the Joint Standard. We understand as per the comments the FSCA has indicated that the definition of "Governing Body" is provided in the Financial Sector Regulation Act, 2017. This should still be inserted on the Joint Standard for ease of reference as the FSCA has done for the definition of 'investment fund administration services' means intermediary services referred to in paragraph (b)(i) of the definition of "intermediary service" as defined in the Financial Advisory and Intermediary Services Act, 2002 (Act No. 37 of 2002), performed in relation to a collective investment scheme or hedge fund. Therefore, the definition in the Joint Standard of "Governing Body" means "governing body as defined in the Financial Sector Regulation Act, 2017." The application of the Joint Standard does not include brokerages or CAT 1 FSP's other than a CAT 1 FSP that provides "investment fund administration services" as part of the definition of "financial institution". The definition does however refer to Insurers. Would this mean that insurers through delegation ensure that brokerages have an adequate cyber risk and cyber resilience policy?	See response to comment 21 above.
23.	SAIA	3. Definition of **Material incident**	The use of the words "material incidents" is broad/ vague. Suggestion is for the word "cyber" to be included to read as "material cyber incident.	The definition of a material incident is standard. In this context however, the material incident is limited to where there is a cyber incident or

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
				information security compromise.
24.	FirstRand	3. Definitions and interpretation **'material incident'** means 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;	We repeat relevant comments submitted in July 2021 through BASA regarding this definition (these have not been noted in the FSCA comment matrix document – pages 9 to 11 - issued in November 2022): 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 23 above.
25.	BASA	3. Definitions and interpretation 'material incident' means 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;	We repeat relevant comments submitted in July 2021 regarding this definition (these have not been noted in the FSCA comment matrix document – pages 9 to 11 - issued in November 2022):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 23 above.
26.	FirstRand	3. Definitions and interpretation **'senior management'** means –	Previous FirstRand comment in July 2021 which is still relevant now and must be resubmitted: • Senior management has not been adequately defined. Given the various flat and hierarchical structures in most financial institutions, senior management is often	The Authorities are of the view that the use of key person in the context in which we require senior management intervention is

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		(a) the chief executive officer or the person who is in charge of a financial institution; (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; (bb) has the capacity to significantly affect the financial standing of a financial institution; and (ii) who oversees the enforcement of policies and the implementation of strategies approved, or adopted, by the governing body;	present/evident in many layers of the organisation. If this is a board mandated responsibility, it must be expressly mentioned. • 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 FSRA? If so, to ensure alignment to the enabling legislation, we recommend linking the definition to the FSRA definition, but contextualizing which category of the FSRA definition is relevant for this standard. Please note the above, implies throughout the standard. We repeat relevant comments submitted in July 2021 through BASA regarding this definition (these have not been noted in the FSCA comment matrix document – pages 9 to 11 - issued in November 2022): "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".	too broad and it is not necessary to include the head of control function for example. The definition of senior management is based on the definition in the Insurance Act and is suitable for the purpose of this Joint Standard.
27.	BASA	3. Definitions and interpretation 'senior management' means – (a) the chief executive officer or the person who is in charge of a financial institution; (b) a person, other than a director or a head of a	BASA commented on this in July 2021, it is still relevant and applicable: □ 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. □ The term "senior management" in this standard contains some elements of the definition of "key person" in the	See response to comment 26 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		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; (bb) has the capacity to significantly affect the financial standing of a financial institution; and (ii) who oversees the enforcement of policies and the implementation of strategies approved, or adopted, by the governing body;	Financial Sector Regulation Act but is not fully aligned. Is the intention for "senior management" to be considered as "key persons" under the FSRA? If so, to ensure alignment to the enabling legislation, we recommend linking the definition to the FSRA definition, but contextualizing which category of the FSRA definition is relevant for this standard. Please note the above, applies throughout the standard.	
28.	ENS	1. Definition of '*investment fund administration services*'	This is a new definition seeking to include administrators of CIS and Hedge funds within the financial institutions who must comply with the standard. Our concern is that the definition of "*investment fund administration services*" cross-references to para b(i) of the FAIS Act which is widely drafted. This may inadvertently capture financial institutions not meant to be captured by this definition. We suggest that only "*administration*" as referenced in para b(i) be cross-referenced in this definition. This is essentially the sub-category of "general administration" proposed by the Conduct of Financial Institutions Bill. See suggested clarification below: **'investment fund administration services'** means administration, being a category of non-discretionary intermediary services referred to in paragraph (b)(i) of the definition of "intermediary service" as defined in the Financial	We note that paragraph (b)(i) is wide and therefore we propose to limit the activity to "administering, maintaining or servicing" as referred to in paragraph (b)(i). See proposed amendment.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			Advisory and Intermediary Services Act, 2002 (Act No. 37 of 2002), performed in relation to a collective investment scheme or hedge fund;	
29.	SAIA	3. Definition of **Cyber threat**	The use of the word "circumstance" is vague/ broad. Suggestion that the word be changed from circumstance to "cyber incident.	The Authority has amended the definition to rather refer to a cyber event.
30.	Guardrisk	3. Definition of **Cyber threat**	The use of the word "circumstance" is vague/ broad. Suggestion that the word be changed from circumstance to "cyber incident".	See response to comment 29 above.
31.	SAIA	3. Definition of **Data**	Data is a collection of facts, while information puts those facts into context. While data is raw and unorganized, information is organized. Information maps out that data to provide a big-picture view of how it all fits together. Therefore, the definition of data as a subset of information seems to be incorrect	We have now aligned to the definition of data in the Electronic Communications and Transactions Act, 2002.
32.	Guardrisk	3. Definition of **Data**	Data is a collection of facts, while information puts those facts into context. While data is raw and unorganized, information is organized. Information maps out that data to provide a big-picture view of how it all fits together. Therefore the definition of data as a subset of information seems to be incorrect.	See response to comment 31 above.
33.	SAIA	3. Definition of **IT Environment**	Does human elements on the definition of IT Environment includes all employees or only technology employees, please specify what is referred to by human elements and IT operations. When reference is made to the IT environment is only limited to the technology and the IT Operations team or is it expanded to also include users configured on that environment in terms of access. For example, does IT environment include a member of the Actuarial team that has system administration rights to allocate access to the system	It includes persons that have access to an institution's information assets.
34.	Guardrisk	3. Definition of **IT Environment**	Does human elements on the definition of IT Environment includes all employees or only technology employees, please specify what is referred to by human elements and IT operations.	See response to comment 33 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			When reference is made to the IT environment is only limited to the technology and the IT Operations team or is it expanded to also include users configured on that environment in terms of access. For example, does IT environment include a member of the Actuarial team that has system administration rights to allocate access to the system.	
35.	Guardrisk	3. Definition of **Material incident**	The use of the words "material incidents" is broad/ vague. Suggestion is for the word "cyber" to be included to read as "material cyber incident"	See response to comment 23 above.
36.	SAIA	3. Definition **Sensitive information**	The impact of loss, misuse, or unauthorised access to or modification of sensitive information is broader than just to the public interest. Suggestion that "direct financial" impact be included in the definition of sensitive information.	Disagree as it refers to adversely impacting on the financial institution.
37.	Guardrisk	3. Definition **Sensitive information**	The impact of loss, misuse, or unauthorised access to or modification of sensitive information is broader than just to the public interest. Suggestion that "direct financial" impact be included in the definition of sensitive information.	See response to comment 36 above.
38.	SAIA	3. Definition of **threat intelligence**	Threat intelligence relates directly to the occurrence of a cyber threat/ breach, we suggest that cyber intelligence be linked back to the occurrence of a cyber threat to contextualize	Threat intelligence in the context of this standard is related to cyber and since threat intelligence is a standard definition, the Authorities are of the view that the definition should not be amended.
39.	Guardrisk	3. Definition of **threat intelligence**	Threat intelligence relates directly to the occurrence of a cyber threat/ breach, we suggest that cyber intelligence be linked back to the occurrence of a cyber threat to contextualize.	See response to comment 38 above.
40.	JSE	3. Definitions and interpretation: 'sensitive information'	In our submission to the draft version of the Joint Standard, the JSE recommended that the definition of 'sensitive information' explicitly includes a reference to 'confidential information' as defined in the Financial Markets Act. While we recognise that the revised definition of 'sensitive information' could be interpreted to include 'confidential information', we	Noted and amended according to the second proposal.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			recommend that the definition of 'sensitive information' is amended as follows: 'sensitive information' means information or data where loss, misuse, or unauthorised access to or modification of could adversely affect the public interest of a financial institution or the privacy to which individuals are entitled, and includes confidential information, as defined and contemplated in the Financial Markets Act 2012 (Act No. 19 of 2012); Or, alternatively – 'sensitive information' means information or data where loss, unlawful disclosure, misuse, or unauthorised access to or modification of could adversely affect the public interest of a financial institution or the privacy to which individuals are entitled	
41.	Marsh	Section 3: Definitions and Interpretation	Suggestion will be to cross reference the definitions with the NIST Glossary of Key information Security Terms.	Some of the definitions are derived from NIST.
42.	SAIA	3. Definitions and interpretation of black, grey, white box testing	It is recommended that the terms and definitions be grouped together for ease of reading. We recommend adding "or cyber event" to the end of the definition. The PA acknowledged the comment however the change was not made	When drafting definition, such must be recorded on an alphabetically basis. The Authorities is thus unable to group these definitions Noted cyber event has been added to the definition of security controls.
43.	SAIS	**3.Definitions and interpretation**	**A. Clarification of the definitions of "cyber event"** The definition should be amended to read as follows: "cyber event" means any observable occurrence in an IT system that might lead to a cyber incident. ~~Cyber events sometimes provide indication that a cyber incident is occurring~~; The current definition reads as if ANY observable occurrence in an IT system is a "cyber event"	The definition of cyber event and cyber incident is from the cyber lexicon. The Authorities are of the view that the definitions do not cause any confusion and these definitions will therefore remain unchanged.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			It should be noted that it is only events that potentially lead to a "cyber incident" that must be classified as a "cyber event". In additional to this we would also require that the definition of Cyber Incident be reviewed. We would suggest the following: '**cyber incident'**– means an ~~cyber~~ event that (a) jeopardises the cybersecurity of an IT system or the information processed, stored or transmitted by the system; or (b) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not; Clarity is required in respect of a cyber event that results in a cyber incident and any other cyber event. **B. Clarification of the definitions of:** The definitions that require clarification are as follows: "**data**" means a subset of information in an electronic format that allows it to be stored, retrieved or transmitted; "**IT asset**" means an asset including software, hardware, internal and external-facing network system that are found in the business environment; "**IT environment**" means the IT components which comprise IT assets, operations and human elements of a financial institution; "**IT systems**" means the integration of IT assets within the IT environment; "**information asset"** means any piece of data, device or other component of the environment that supports information-related activities. In the context of this Joint Standard, information assets include data,	The definition of data has been amended to align with the definition in the Electronic Communications and Transactions Act, 2002. The IT environment is where the IT systems operates and it includes operations and human elements. The Authorities are of the view that the use of IT systems and IT environment in the Joint Standard are correct and should not cause any confusion. IT assets definition is broader that information assets and includes information assets.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			hardware and software and excludes paper-based information; **Comments** 1. The definition of "IT environment" already includes "IT assets". However, "IT systems" refers to the "integration" of "IT assets" within the "IT environment". It is unclear what the difference between "IT environment" and "IT systems" is. These terms are not always used consistently through the Joint Standard, which creates room for confusion and incorrect application of the standard. 2. The definition of "information asset" includes "hardware" and "software" which is also included in the definition of "IT asset". It is unclear what the difference between "information asset" and "IT asset" is. It is proposed that these definitions be clarified so as to ensure they do not overlap and can be consistently applied throughout the Joint Standard. **C. Definition of "information asset"** Subject to the changes required in terms of A above (Clarification of the definitions of "cyber event"), a simplification of the definition is proposed, as indicated below: "**information asset"** means any ~~piece of~~ data, hardware, software, device or other component of the IT environment that supports information-related activities, but in the context of this Joint Standard, information assets ~~include data, hardware and software and~~ excludes paper-based information;	Based on the aforementioned, the amendment proposed here does not substantially change the definition.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			Consistency and alignment is required to ensure no confusion and a consistent application of the standard to achieve the desired outcome.	
44.	WTW (Willis Towers Watson)	3 (Definitions and Interpretation) - Definition of **"financial institution"** As an aside, we point out that "captured financial institutions" is perhaps an unfortunate choice of words. We realize that, if a financial institution does not operate any of its own IT systems, then very many of the listed items cannot be directly applicable to it, although it would be desirable for the institution to ensure that its critical service providers comply – applying the approach suggested in para 8.6.1(b).	We note that this now includes as item (k), "*an administrator approved in terms of section 13B of the Pension Funds Act*". **We welcome this,** although we note that in the Comment Matrix (at no.39), the response to this suggested inclusion is actually "*Although we agree with your proposal in principle, the Authorities are concerned that extending the scope of the Joint Standard would constitute quite a material change that was not consulted on previously. Accordingly, the Authorities will not address the proposal at this stage...*".	Noted.
45.	WTW (Willis Towers Watson)	3. Definition of **"material incident"**	**We welcome this**, but please note our comment in Section C below.	Noted.
46.	WTW (Willis Towers Watson)	3. Definition of **"sensitive information"**	A minor point, but is the wording change from "public interest or a financial institution or the privacy…", to "public interest of a financial institution or the privacy…" deliberate?	Noted and amended accordingly.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
47.	Aurora Insurance	4.Application	Duly noted. Our Cybersecurity framework has been designed to reflect the nature, size, complexity and risk profile of our company and is enhanced continuously.	Noted.
48.	SAIS	**4. Application**	The SAIS refers to the application of the standard and the absence of the term "authorised user," (AU) as defined in section 1 of the Financial Markets Act 2012 (Act No. 19 of 2012). The definition of a "financial institution" in the Joint Standard requires further clarity. AUs play an integral part in South Africa's financial eco system and as a general principle, one would expect AUs to be included in the Joint Standard. The SAIS' assumption is that the FSCA views the market infrastructures i.e. exchanges, as being responsible for the regulation and implementation of the standards for AUs. However, this approach raises a problem, as AUs can be members of multiple exchanges. Requiring exchanges to oversee the implementation of the Joint Standard for AUs could lead to varying interpretations and implementation of the standards between: - The Financial Services Conduct Authority and the exchanges; and - Between the different exchanges themselves. It is proposed that exchanges have a consistent approach to the implementation of the Joint Standard as it relates to AU's. Furthermore, that this approach is set by the FSCA to ensure alignment with other financial institutions, as is required, to comply with the standard. As mentioned above, it is important to consider the fact that many AUs are also Financial Services Providers (FSPs)	Firstly, the Standard is applicable to financial institutions as defined. Therefore, the authorised users are not contemplated in the definitions of a financial institution in terms of this Standard. The definition of a financial institution was carefully crafted to include a specified financial institution, taking into consideration how onerous these requirements are. Secondly, market infrastructures must comply with the requirements of the Standard. Therefore, a market infrastructure is ultimately responsible for complying with the requirements in the Standard. Notwithstanding the above it is incumbent upon a market infrastructure to ensure that the third parties it engages with or outsource certain functions, have the requisite operational ability which will include the necessary cyber resilience and cyber frameworks. This

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			and therefore are dually regulated i.e. by the FSCA and exchanges. The SAIS would want to ensure that the requirements applicable to AUs are standardised so as to guarantee that there are no inconsistencies in the application of the requirements relevant to AUs and those applicable to FSPs. To address this issue, the SAIS proposes the following alternative: - Insertion of a clause stating that an AU who is also a registered FSP shall be exempt from regulatory oversight by the exchange, as they are already supervised by the FSCA in accordance with their FSP license. With the impending COFI amendments due to be released shortly for comment, the market is uncertain of where the regulation of AUs will fall. It is imperative that the impact and the possible practical issues that could arise in relation to the licencing and supervision of AUs remain top-of-mind. Regulation must be streamlined to ensure that the objectives of COFI and other Codes of Conduct and Standards be aligned. This is to ensure that there is regulatory interoperability and thereby making certain that no regulatory arbitrage and duplication of requirements occurs creating unlevel playing fields and possible parries to entry.	can be dealt with in the exchange rules if necessary. Thirdly, the FSCA is also considering whether it should develop a cross cutting Standard that will apply to other financial institutions not contemplated in the Joint Standard, which may possibly include authorised users. Fourthly, for the reasons stated in the preceding paragraph, we disagree with the proposal to insert a clause in respect of authorised users. Finally, with regards to the COFI Bill developments and authorised users, the COFI Bill will introduce an activity-based regulatory framework. An entity will have to consider the activities that it performs and whether those fall within the activities listed in Schedule 2 of the COFI Bill. The Authorities are mindful of the need to ensure alignment of regulation, minimize duplication and reduce regulatory arbitrage.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
49.	Assupol	4.1	No comment	Noted
50.	Assupol	4.2	No comment	Noted
51.	ASISA	4.2	The recommendation is to replace the word *"mitigated"* with ***"managed"*** as not all risk exposures can be mitigated (considering that there are other risk response strategies in risk management i.e., the acceptance of risk, the transfer of risk, and the avoidance of risk): …….. are catered for and ~~mitigated~~ **managed** in the application of the …….	The Authorities disagree, mitigation is the correct word to be used in this context.
52.	ASISA	4.3	It is proposed to insert the word *"**an**"* before *"insurer"* to read as follows: A financial institution that is **an** insurer or the controlling ……	Noted. 'An' was added before 'insurer'.
53.	Assupol	4.3	No comment	Noted.
54.	Assupol	4.4	The standard has been clarified to refer to minimum requirements and principles and welcome the reduced scope that limits application to risk profile. The clarification adopts a revised standard from minimum requirements for sound practices and processes.	Noted.
55.	Marsh	Section 4: Application, bullet point 4.4	4.4 Rather end the sentence after the word "implemented". The remainder of the sentence causes undue confusion. Either you implement the minimum control or not, else this standard is to be used at discretion.	The Authorities disagree as the remainder of the sentence deals with proportionality.
56.	FirstRand	4. Application 4.1. This Joint Standard applies to financial institutions as defined in this Joint Standard. 4.2 A financial institution that is a bank, or a controlling company	Can the standard also apply to organisations that fall under the classification of National Payment System (NPS) and Financial Market Infrastructures (FMIs) including organisations such as clearing houses (BankservAfrica and the RTGS/SAMOS). This could help consolidate the draft policy requirements contained in the new SARB NSPD consultation paper on cyber resilience.	Note that payment providers are not currently regulated by the Prudential Authority. Although the FSCA has been given jurisdiction over payment providers from a conduct perspective, the FSCA has not started to

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		must ensure that any risks relating to cybersecurity and cyber resilience from juristic persons (both local and foreign) 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.		formally regulate payment providers. Including payment providers in the scope of this Joint Standard is therefore premature. With regards to market infrastructures, they are currently included in the scope of the Joint Standard- see paragraph (e) of the definition of financial institution in the Joint Standard.
57.	BASA	4. Application 4.1. This Joint Standard applies to financial institutions as defined in this Joint Standard. 4.2 A financial institution that is a bank, or a controlling company must ensure that any risks relating to cybersecurity and cyber resilience from juristic persons (both local and foreign) and branches structured under the bank or the controlling company, including all	Can the standard also apply to organisations that fall under the classification of National Payment System (NPS) and Financial Market Infrastructures (FMIs) including organisations such as clearing houses (BankservAfrica and the RTGS/SAMOS). This could help consolidate the draft policy requirements contained in the new SARB NSPD consultation paper on cyber resilience.	See response to comment 56 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		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		
58.	BASA	4.5 "Where words such as 'appropriate, adequate, effective, timely, regular, or periodic' are used in this Joint Standard, the implementation of the relevant requirement must be assessed in consideration of the nature, size, complexity and risk profile of a financial institution."	For Cybercrimes, is there guidance for the assessment of the risk profile? FAIS impacted FSP's and the products which we sell are segmented under Tier 1 and Tier 2. For FICA, consideration in relation to the type of industry, products, transactional behaviour, jurisdiction etc. is considered, when assessing the risk profile of an FSP. Are there any additional requirements that this joint standard imposes?	No, not at this stage. Institutions are expected to develop their own risk appetite, risk framework based on their risk profile in consideration of the minimum requirements of this Joint Standard.
59.	ENS	4.4 and 4.5	In response to our **everything OK stop** earlier comment on proportional application of the Joint Standard the Authorities indicated that the "the Joint Standard prescribed minimum requirements and principles on the subject matter and the expectation is that all captured financial institutions must comply". Para 4.4 now references the minimum requirements and principles set out in this Joint Standard but requires that they must be implemented to reflect the nature, size, complexity and risk profile of a financial institution. We assume that this is a reference to all of the requirements set out in the Joint Standard. We continue to believe that this is very onerous for small financial institutions. Para 4.5 then provides that where words such as "*appropriate, adequate, effective, timely, regular, or periodic"*	The Joint Standards contains the minimum requirements that must be implemented by all financial institutions. With regard to larger financial institutions, the minimum requirements may not suffice to meet the actual risks. Therefore, when conducting supervisory reviews, the Authorities may assess controls and processes in respect of the nature, size, complexity and risk profile of the institution. In the example

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			are used in this Joint Standard, the implementation of the relevant requirement must be assessed in consideration of the nature, size, complexity and risk profile of a financial institution. In our view this results in ambiguity. Does this mean that (i) only where the words "*appropriate, adequate, effective, timely, regular, or periodic"* are used may a financial institution assess the level of implementation required of the minimum requirement or principle, or (ii) does para 4.4 prevail with the effect that a financial institution may always assess implementation of the principles and minimum requirements of the Joint Standard on the basis of its nature, size, complexity and risk profile? If the latter then para 4.5 is misleading and should be amended. If a financial institution is empowered to make an assessment when implementing all of the minimum requirements and principles it remains unclear *how* this assessment is to be made by a financial institution. For example, could a small financial institution elect not to establish a function responsible for cyber and information security (as required by para 6.1.3) on the basis that its governing body will, given the size of the financial institution, fulfil this role or is the correct interpretation rather that such function must be established (as this is a minimum requirement) and the only flexibility is the extent of the resources which will be attributed to that function, presumably it should always have appropriate authority if established. Clarity on the way in which this assessment should be made by a financial institution is critical as the governing body of the financial institution is ultimately responsible for ensuring compliance by the financial institution (in terms of para. 5.1.1) with the requirements set out in the Joint Standard and will	provided in terms of the establishment of a function responsible for cyber and information security, the function must be established, but the extent of the resources to capacitate the function will depend on the nature, size, complexity and risk profile of the financial institution.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			need to know how to manage the risk of this liability and ensure compliance.	
60.	FIA	4.2 and 4.3	"Any risk relating to cybersecurity and cyber reliance" is an endless statement. The definition of a Cyber Risk in section 3 is also too broad of a definition. Probability and impact need to be defined in such a manner as to be clear and precise to prevent confusion	Any risk in relation to cyber security and cyber resilience has the potential to cause devastating impact on the financial soundness of the financial institution and its customers. The definition of Cyber Risk is from the FSB Cyber Lexicon which is commonly understood and accepted.
61.	FIA	4.4 and 4.5	- Lack of a definition of recognised standard (e.g. NIST or ISO 27000 series) means that whether employing human assets in the Cyber Security role OR contracting to a third party, a new "strategy" will need to be researched to meet the needs of this new standard vs. being able to implement an existing proven strategy. This is an evolving space with the threat landscape changing daily but without a reasonable and recognised start point, it will take months of consulting the "Revised Joint Standard – Cybersecurity and Cyber Resilience" to build a suitable framework and this is before implementation and testing. o There is mention of the Revised Joint Standard – Cybersecurity and Cyber Resilience being in line with best practice, which is true, but it still lacks enough conformity to align with a widely recognised standard that can be adhered to, to avoid non-compliance and leaves an opening for interpretation and creates a large litigation risk.	The Joint Standard is derived from internationally recognised standards such as NIST, ISO, CPMI-IOSCO etc.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
62.	FirstRand	4.5 "Where words such as 'appropriate, adequate, effective, timely, regular, or periodic' are used in this Joint Standard, the implementation of the relevant requirement must be assessed in consideration of the nature, size, complexity and risk profile of a financial institution."	For Cybercrimes, is there guidance for the assessment of the risk profile? FAIS impacted FSP's and the products which we sell are segmented under Tier 1 and Tier 2. For FICA, consideration in relation to the type of industry, products, transactional behaviour, jurisdiction etc. is considered, when assessing the risk profile of an FSP. Are there any additional requirements that this joint standard imposes?	See response to comment 58 above.
63.	WTW (Willis Towers Watson)	4.4 and 4.5	We note that numerous comments were made on para. 3.5 of the first draft Joint Standard, and we note the Authorities' responses to these in the Comment Matrix (items 15 to 24). We are not convinced however that 4.4 and 4.5 provide sufficient clarity – e.g. we note the response to comment 24 includes "*The Joint Standard prescribed minimum requirements and principles on the subject matter and the expectation is that all captured financial institutions[1] must comply.*" (But comply with what? – 4.4 and 4.5, or the 100-or-so listed items prefaced with "*A financial institution must…*"?)[2] We noted previously that only a few of the very largest pension funds operate their own IT infrastructure. For the vast majority, critical services are outsourced to professional service providers such custodian banks, investment managers, and Section 13B administrators. It would seem reasonable and proportionate to us to require the Trustees of such pension funds to make periodic enquiries of their key	Comments noted. 1.The Standard is drafted in a principles-based manner. Further, when drafting the Standard, the Authorities considered the implications of the Standard on smaller entities. 2.In this light, in terms of all the requirements in the Standard, paragraphs 3.4 and 3.5 enables proportional application of the Standard. 3. In addition, in order to ease regulatory burden, there are

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			service providers as to their level of compliance with the Joint Standard (including some detail on their cyber-resilience measures and protections, and also on their liability insurance), but to go little further than that if the responses are satisfactory. (Service provider contracts should also include suitable requirements and protections for the pension fund, in line with para 5.2.3 – this is reasonable.) We **think** this is consistent with para.s 4.4 ("*minimum requirements and principles … must be implemented to reflect the nature, size, complexity and risk profile…*") and 4.5, but we seek confirmation of this, ideally with some expansion of paras 4.4 and 4.5 to give extra clarity. We also point out that it is not very helpful simply to say "*Smaller financial institutions must approach the PA when they are concerned with their compliance with the Joint Standard*" (response to no.18 in the Comment Matrix), or "*Exemptions are dealt with in terms of the provisions of section 281 of the FSR Act*" (response to no.24) – there are hundreds of "smaller financial institutions". Does the PA really want these to approach it individually, or seek individual exemptions? Would it not be better to provide more clarity on these matters upfront? ("More clarity" could just be supplementary guidance issued together with the Joint Standard.)	specific supervisory and regulatory interventions available to smaller entities. For example, the Authorities can therefore adopt a "lighter touch" approach when supervising these requirements in respect of smaller institutions. 4.With regards to outsourcing of IT infrastructure and critical services to third party providers, please note that a financial institution may outsourced such functions as it deems necessary. However, a financial institution must ensure that roles and responsibilities are clearly defined in the contract or Service Level Agreement with third-party service providers. Further, notwithstanding any outsourcing of functions, the financial institution remains ultimately accountable for complying with the requirements in this Standard. 5. With regards to the balance of the comments and for completeness please note that it is beyond the scope of this Standard to detail how

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
				the requirements will be tested or implemented. The Authorities can supplement the Standard with a Guidance to provide more detail. In addition, there is a proportional application of the Standard as per paragraphs 3.4 and 3.5. Further, supervisory and regulatory discretionary will be exercised when monitoring implementation of the Standard.
64.	Marsh	Section 4: Application, bullet point 4.6	Rather remove the words “financial sector” as there are some laws and Act’s that are applicable across sectors, e.g. Cyber Crimes act	A financial institution should comply with all legislation applicable to them. The Authorities are, however, only concerned with the compliance with financial sector laws as listed in Schedule 1 of the FSR Act, as these laws fall within the jurisdiction of the Authorities.
65.	Aurora Insurance	5. Roles and Responsibilities	Duly noted.	Noted.
66.	Assupol	5.	No comment	Noted.
67.	Marsh	Section 5: Roles and Responsibilities bullet point 5.1	Provide a definition for Governing Body in the definitions section.	Disagree. See response to comment number 21 above.
68.	SAIA	5.1.2 The governing body is ultimately responsible for the oversight of	Clarity is sought as to whether the delegation to senior management committees is acceptable alternatively whether the standard is referring to Board Committees such as Audit and Risk Committee?	The board is ultimately responsible and accountable for compliance with the Joint Standard to the Authorities.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		cyber risk management but may delegate primary oversight activities to an existing or new committee.		Delegation may occur as the board deems fit.
69.	SAIA	5.2.3 ensure that roles and responsibilities for security are clearly defined in the contract or Service Level Agreement with third-party service providers.	Clarity is sought as to whether this covers all third parties or specifically to Information Technology third parties. We would recommend that the timeframe to comply be extended to 24 months as challenges may be experienced in covering all third parties within 12 months due to the utilization of various systems across third parties.	The Joint Standard covers all third parties that have access to the institution's information assets, however, institutions can apply for extension to comply in terms of section 279 of the FSR Act.
70.	Batseta	5.4 and 5.15	Batseta supports: 5.4 A 12-month transitional period following the publication of the Joint Standard. Considering the burden on principal officers and trustees a phased approach is suggested given that retirement funds are still dealing with recent compliance requirements. 5.15 The extension of the Joint Standard to credit rating agencies, benefit administrators and Category 1 FSP's that provide investment fund administration services. These types of service providers are regularly contracted by retirement funds.	Noted.
71.	Aurora Insurance	6.Governance	Duly noted. Our Governance framework has been designed to reflect the nature, size, complexity and risk profile of our company and is enhanced continuously.	Noted.
72.	Batseta	6	Application: Batseta is of the view that the FSCA should include compliance with the Joint Standard as part of the licencing requirements. This will ensure that pro-active measures are in place to prevent and/or mitigate the risks associated with cybersecurity.	Disagree with the comments. The FSCA as part of assessing applications for a license do consider operational ability of applicants which may include

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
				operational resilience and IT Governance and Cybersecurity and Resilience.
73.	SAIS	**6. Governance**	In the definition of "senior management" (control function) and in the following clauses: • 5.1.2 (committee); • 6.1.1 (committees and oversight functions); • 6.1.3, (functions); • 6.1.4 (functions); and • 6.2 (independent oversight function), there are various references to ""function"; "oversight function" and "committees". There is a requirement for a "**function** responsible for cyber and information security" (clause 6.1.3). Then there is a requirement for **oversight of the function** (clause 6.1.4). Then the Authorities may require **independent oversight function** (clause 6.2), *however* clause 5.1.2 allows a governing body to delegate oversight to a **committee** To clarify the different roles it is proposed that there should be reference to a "function" (clause 6.1.3), but that any reference to the oversight of the function make reference to a "committee" (e.g. clauses 6.1.1, 6.1.4, 6.2). Proposed changes: 6.1.1 clearly define the roles and responsibilities of all management and ~~oversight~~ functions (including lines of defence) as well as committees established for the purposes of exercising oversight ~~of cyber risks~~; 6.1.4 ensure that the committee that exercises oversight of the function(s) referred to in subparagraph	The Joint Standard does not have requirements relating to delegation. Ultimately the financial institution must determine delegation to different functions and committees. The board is responsible for compliance with this Joint Standard. Due to the various types of financial institutions in scope in this Standard we cannot insist that certain matters have committee oversight as some institutions may not have such committees. The Authorities do not support the proposal. The one is in reference to operation and the other is in reference to control functions. Agree, see amendments made to the Standard. Comments noted. Please note that the Standard is drafted in an outcomes and principles based manner and

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			6.1.3, has access to the governing body, is structured in a manner that ensures adequate segregation of duties and avoids any potential conflicts of interest. 6.2 In reference to subparagraphs 6.1.3 and 6.1.4, the Authorities may require a financial institution, based on its nature, scale, complexity and risk profile, to have an independent oversight committee ~~function~~. **Access to the/a governing body** Both clauses 6.1.2 and 6.1.4 contain the requirements for "direct reporting lines" (clause 6.1.2) and "has access to the governing body" (clause 6.1.4). It is proposed that this requirement to be consolidated in clause 6.1.4 and the following change to clause 6.1.2 be made: 6.1.2 ensure cyber risk management is 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~~; Staff and management have access to the oversight (independent oversight) committee which in turn has access to the governing body. The SAIS notes that governance structures will vary depending on the size, nature and complexity of the business as is required by the Joint Standard. This may result in different ways of ensuring governance of the Joint Standard e.g. smaller entities may not have separate IT Risk, Governance Committees but will deal with this an all-encompassing item within existing management structures.	not as a one size fits all instrument. The unintended consequences of what is proposed in this comment may result in a rigid, tick box application of the requirements and supervisory inflexibility. We submit this is not a desirable outcome.
74.	SAIS	**6.1** A financial institution must	Financial entities such as category II FSPs may have white labelling arrangements with other FSPs such as collective investment schemes and/or co-branding arrangements. It is	Comment noted. See comments above at item 63. The definition of a "financial

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			unclear as to where the accountabilities for the ownership of a framework lie, as each of the cyber threats may reside in separate areas of the agreement. Said agreements are specific in terms of market conduct related responsibilities under the Retail Distribution Review. As mentioned above, this cannot be looked at in isolation and must be considered in light of COFI.	institution" in the Standard was carefully crafted to include entities who, due to their role within the financial ecosystem, are highly vulnerable to cyber threats. Each entity contemplated in the Standard, is responsible for complying with the requirements. It is beyond the scope of this Standard to demarcate and delineate the roles and responsibilities of the various role player within the cyber value chain. Suffice to say the Standard provides overarching principles and requirements and applies to the financial institutions listed in the Joint Standard.
75.	Assupol	6.1	6.1.3 Note the expansionary application from information security to now include both information security and cyber security. This does not affect how Assupol will respond to the standard as we do not have an internal distinction. 6.1.4 We welcome the amendment from direct reporting lines to access to governing body. This does not affect how Assupol will report and communicate to the governing body.	Noted.
76.	Marsh	Section 6 Governance bullet point 6.1.3	Consider providing a definition of "function"	The Authorities are of the view that it is not necessary to define function in the Joint Standard. We would, however, regard 'function' to include a person or a unit with specific responsibility in the subject matter required.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
77.	SAIA	6.1.3 A financial institution must ensure cyber risk management is 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.	Please clarify what does the last sentence mean, "including provisions relating to direct reporting lines to the governing body" It is recommended that the sentence be reworded to: *A financial institution must ensure cyber risk management is incorporated into the governance and risk management structures, processes, and procedures of a financial institution. A direct reporting line to the Governing body should be established in terms of the Governance Framework.*	Agreed. The Joint Standard has been amended accordingly.
78.	SAIA	6.13 A financial institution must – 6.1.3 ensure that a function(s) responsible for cyber and information security is established with adequate resources and appropriate authority. 6.1.4 ensure that the oversight of the function(s) referred to in subparagraph 6.1.3, has	Clarity is sought as to whether the standard is requiring structural changes to the reporting lines of the CIO directly into the Governing Body and the information security functions reporting line away frm the Chief Information Officer. It is our understanding on the reading of this section that the oversight (provided by internal audit and 2nd line Compliance) of this function should have a direct reporting line to the governing body. The oversight being referred to may include Compliance, Risk and Audit. It is our respectful submission that if this is the correct reading of the requirement, that it be articulated clearly to avoid misinterpretation.	The Standard is requiring additional reporting lines. Paragraph 6.1.4 has been amended to include control functions.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		access to the governing body is structured in a manner that ensures adequate segregation of duties and avoids any potential conflicts of interest.		
79.	SAIA	6.1.3 With reference to subparagraphs 6.1.3 and 6.1.4, the Authorities may require a financial institution based on its nature, scale, complexity and risk profile to have an independent oversight function.	As per comment above. Would this be referring to an external auditor?	This section is referring to the control functions and not to the external auditor. The paragraph has, however, been amended to include control functions to make it clearer.
80.	Outsurance	6.1.4	We kindly request clarity on the amended section in the revised draft standard. The current paragraph is unclear and it appears as if there is some wording missing. Is the section meant to read as follow: "ensure that the oversight of the function(s) referred to in subparagraph 6.1.3, has access to the governing body **and** is structured in a manner that ensures adequate segregation of duties and avoids any potential conflicts of interest."	Noted. See response to comment 78 above.
81.	ASISA	6.1.4	It is proposed to insert the word ***"and"*** after the word *"body"* to read as follows*:* ……. access to the governing body **and** is structured in a manner …….	Noted. See response to comment 78 above.
82.	Assupol	6.2	No comment	Noted.
83.	ENS	6.2	Please clarify how the Authorities would require a financial institution to contract an independent cyber and information	During the course of our supervisory interventions the

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			security function in accordance with this empowering paragraph. Would this be by way of a directive issued to a particular financial institution or a class of financial institutions? The requirement for an independent function would impose additional costs on the financial institution and so in order to ensure equal treatment should not be imposed on a specific financial institution and not others in a class of financial institutions.	specific institutions will be identified and notified bilaterally.
84.	Aurora Insurance	7.Cybersecurity strategy and framework	Duly noted. Currently our Cybersecurity strategy and framework has been incorporated based on our nature, size, complexity and risk profile of our company and is enhanced continuously.	Noted.
85.	MMI	7.1 Vulnerability assessment	The current definition of "vulnerability assessment" is inconsistent with the generally accepted definition and may be confused with a "risk assessment". This is because a "risk assessment" includes "a systematic review of controls and processes", this is not done in a vulnerability assessment, which usually just looks for vulnerabilities in a system. We would recommend using the NIST definition: "Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation."	See response to comment 15 above.
86.	FirstRand	7.1. A financial institution must – 7.1.1 establish and maintain a cybersecurity strategy that is approved by the governing body and aligned with its overall business strategy;	Previous FirstRand comment in July 2021 which is still relevant now and must be resubmitted: • "Frequency of review 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". • We therefore suggest that the phrase "but at least annually" in sub-clause 7.1.2 should be deleted.	Generally strategies are reviewed annually. Due to the evolving nature of this topic, the Authorities are strongly of the view that review must be done at least annually. The Authorities are being specific with this requirement because of the nature of this risk.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		7.1.2 **review the cybersecurity strategy regularly, but at least annually**, to address changes in the cyber threat landscape, allocate resources, identify and remediate gaps, and incorporate lessons learnt;		
87.	BASA	7.1. A financial institution must – 7.1.1 establish and maintain a cybersecurity strategy that is approved by the governing body and aligned with its overall business strategy; 7.1.2 review the cybersecurity strategy regularly, but at least annually, to address changes in the cyber threat landscape, allocate resources, identify and remediate gaps, and incorporate lessons learnt;	BASA commented on this in July 2021, it is still relevant and applicable: □ "Frequency of review will vary amongst institutions; hence BASA recommends that the second sentence be amended to "…reviewed regularly in accordance with the financial institutions internal processes to ensure relevance and appropriateness". We therefore suggest that the phrase "but at least annually" in sub-clause 7.1.2 be deleted. □ The Joint Standard requires a Financial Institution to have adequate cybersecurity and cyber resilience measures in place. The proposed Joint Standard sets out the requirements for sound practices and processes of cybersecurity and cyber resilience for financial institutions. Has the provisions of the Cybercrimes Act and the requirements placed on Financial Institutions to identify and report Cybercrimes etc. been considered, so that there is an alignment and a complete overview on the requirements for both the Joint Standard and the Cybercrimes Act incorporated into the adequate cybersecurity and cyber resilience measures that must be in place and prevent a duplication relating to cyber risks?	See response to comment 86 above. During December 2021 there was questionnaires released relating to the impact of this Joint Standard on financial institutions. Kindly refer to the statement of need for intended operation and expected impact.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
88.	BASA	7.1.5. establish cybersecurity policies, standards and procedures that are informed by industry standards and best practices to manage cyber risks and safeguard information assets, taking into consideration the evolving technology and cyber threat landscape;	Do the policies need to be separate or is it sufficient if the principles are included in combined policies that can logically be grouped? The requirement codifies the establishment of policies, standards and procedures informed by industry standards. As the standard applies to different financial institutions, there may be inconsistencies in specific sector industry standards, therefore the requirement to align with industry standards could result in inconsistencies in compliance with the standard. Further, requirements must be applied proportionally to the risk profile of the financial institution with the result that these may not be aligned with industry standards.	As long as the policies are identifiable in terms of the requirements of the Standard.
89.	Marsh	Section 7: Cybersecurity Strategy and framework bullet point 7.1.5	Consider adding processes to this list of artefacts	Noted and amended accordingly.
90.	Marsh	Section 7: Cybersecurity Strategy and framework bullet point 7.1.6	Consider providing a recommended frequency instead of the word Regularly	With reference to paragraph 4.5 of the Joint Standard, where words such as ‘appropriate, adequate, effective, timely, regular, or periodic’ are used in this Joint Standard, the implementation of the relevant requirement must be assessed in consideration of the nature, size, complexity and risk profile of a financial institution.
91.	Assupol	7.1	7.1.6 Note the amendment from the fixed time-line (annually) to ad-hoc interval (regularly). There has also been an amendment in the standard from define and quantify, to define and reassess. This amendment is welcome as it aligns with Assupol processes.	Noted.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			7.17 Note the amendment in standard from the conservative gather to the more active track and manage. This will not affect how Assupol's cyber security strategy and framework.	
92.	Outsurance	7.1.7	The change does not appear to be in line with the changes in the comment matrix and "enable" has not been changed to "inform" to address the fact that not all metrics enable reporting on the draft standard.	Noted and amended accordingly.
93.	Assupol	7.2	Note the review body has been amendment from the compliance and audit function to specifically an independent review function. Assupol will align to the revised standard.	Noted.
94.	SAIS	**7.2** The cybersecurity framework must	The question is raised as to how the FSCA envisages accountability for outsourcing providers. Clarity is required as to whether any recourse for an IT vendor's accountability for introducing cyber threats through negligence be managed via litigious processes and not via the regulators. The SAIS is of the opinion that an IT vendor is a responsible party in respect of the IT and cybersecurity and as such should be regulated accordingly. FSCA should consider the IT vendors as applicable parties to this Joint Standard to mitigate further IT Risks.	It remains the ultimate responsibility of the financial institution. The contract is between the financial institution and the third party and the provisions relating to recourse should be specified in the contract.
95.	Marsh	Section 7: Cybersecurity Strategy and framework bullet point 7.2.2	Consider just prescribing the review being done annually, as most companies will default to the mandatory prescription à at least annually.	The Authorities prescribes that the review must be conducted at least annually, however, the institutions are not limited to one review per year, it can be done regularly based on the risk profile of the institution.
96.	BASA	7.2 The cybersecurity framework referred to in subparagraph 7.1.3 must –	A "framework" is not subject to either "annual" or "independent" review, particularly in a large conglomerate. Reviews will be undertaken regularly, but not annually and these evaluations are conducted internally by either Internal Audit or independent monitoring teams.	See response to comment 95 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		7.2.1 be approved by the governing body; 7.2.2 be reviewed regularly, but at least annually, for adequacy and effectiveness through an independent review; and 7.2.3 clearly articulate how a financial institution will identify cyber risks and determine the controls required to keep those risks within acceptable limits.	We suggest that Clause 7.2.2 be reworded as follows: "7.2 The cybersecurity framework referred to in subparagraph 7.1.3 must – 7.2.1 be approved by the governing body; 7.2.2 be reviewed regularly, but at least annually, for adequacy and effectiveness through an independent review; and 7.2.3 clearly articulate how a financial institution will identify cyber risks and determine the controls required to keep those risks within acceptable limits."	The Authorities are not in support. Refer to the definition of independent review in the Joint Standard. The review can be conducted by an internal or external audit function or an independent control function.
97.	FirstRand	7.2 The cybersecurity framework referred to in subparagraph 7.1.3 must – 7.2.1 be approved by the governing body; 7.2.2 **be reviewed regularly, but at least annually**, for adequacy and effectiveness **through an independent review**; and 7.2.3 clearly articulate how a financial institution will identify cyber risks and determine the controls	• A "framework" is not subject to either "annual" or "independent" review, particularly in a large conglomerate. Reviews will be undertaken regularly, but not annually and these evaluations are conducted internally by either Internal Audit or independent monitoring teams. • We suggest that Clause 7.2.2 should be reworded as follows: "7.2 The cybersecurity framework referred to in subparagraph 7.1.3 must – 7.2.1 be approved by the governing body; 7.2.2 **be reviewed regularly, ~~but at least annually~~**, for adequacy and effectiveness **~~through an independent review~~**; and 7.2.3 clearly articulate how a financial institution will identify cyber risks and determine the controls required to keep those risks within acceptable limits."	See response to comment 96 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		required to keep those risks within acceptable limits.		
98.	SAIA	7.2.2	It may not be practical to perform an independent review of the adequacy and effectiveness of the cyber security framework annually. This review would have very wide scope and would require extensive resources to complete. It may be more practical to perform a review of the adequacy and effectiveness of the framework every 3 years.	The Authorities do not support a 3-year review. Refer to the definition of independent review in the Joint Standard. The review can be conducted by an internal or external audit function or an independent control function.
99.	Guardrisk	7.2.2	It may not be practical to perform an independent review of the adequacy and effectiveness of the cyber security framework annually. This review would have very wide scope and would require extensive resources to complete. It may be more practical to perform a review of the adequacy and effectiveness of the framework every 3 years.	See response to comment 98 above.
100.	MMI	7.2.2	It may not be practical to perform an independent review of the adequacy and effectiveness of the cyber security framework annually. This review would have very wide scope and would require extensive resources to complete. It may be more practical to perform a review of the adequacy and effectiveness of the framework every 3 years.	See response to comment 98 above.
101.	ASISA	7.2.2	The adequacy and effectiveness of the cyber security framework, in general, do not require changes as regular as annually. Such a review has a wide scope and require extensive resources to complete and it might be more practical to perform such a review of the framework at least once every 3 years. A review of the cyber security controls however, could be perform on an annual basis. It is proposed to change the wording as follows:	See response to comment 98 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			"be reviewed ~~regularly, but~~ at least ~~annually,~~ **every 3 years** for adequacy and effectiveness through an independent review. **The adequacy and effectiveness of the cyber security controls must be reviewed through an independent review at least annually;** and"	
102.	ENS	7.2.2	Please clarify what would constitute an independent review of a cybersecurity framework.	It will be a review done by an independent person. Refer to the definition of independent review in the Joint Standard
103.	Aurora Insurance	8. Cybersecurity and cyber-resilience fundamentals	8.1. Identification – Duly noted. Our monthly risk assessments are aligned with this. 8.2. Protection – Duly noted. The acquisition of an Intrusion Detection System has not been finalised due to the restrictive cost implications. Monitoring and Training components already form part of our Cybersecurity framework. 8.3. Detection – Duly noted. We are expanding our investigations into related logs. 8.4. Response and recovery – Duly noted. More robust Cyber Drill simulations are being investigated. 8.5. Situational awareness – Duly noted. We are continuously enhancing our Cyber Threat Intelligence gathering process. 8.6. Testing – Duly noted. Identifying appropriate threat simulation software is high on our agenda but availability and costs may be prohibitive. 8.7. Learning and evolving – Duly noted. Our Cybersecurity framework allows for application of lessons learnt from previous events.	Noted.
104.	Assupol	8.1	8.1.1 Note specified security risk assessment 8.1.2 Note the amendment in frequency of review to regularly and at least biennially. Assupol will align to this timelines.	Noted.
105.	SAIS	**8.1** Identification	It is unclear why this section covers only "information assets" and not "IT assets".	Please note that the definition of information asset in the

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			8.1.1 A financial institution must – (a) identify business processes, IT assets and information assets that support business and delivery of services, including those managed by third-party service providers; (b) in reference to item (a), classify the business processes, IT assets and information assets in terms of criticality and sensitivity, which in turn must guide the prioritisation of its protective, detective, response and efforts (c) carry out security risk assessments on its critical operations, IT systems and ~~supporting~~ information assets to be protected against compromise as well as external dependencies, in order to determine the priority; and [clarity is required in respect of what supporting information is] (d) maintain an inventory of all its IT assets, information assets which includes location, ownership, the roles and responsibilities of managing the information assets.	Joint Standard has been amended to include IT asset. The 'supporting' has been deleted from (c).
106.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.1.1 (c)	Would information assets be assigned roles ?	Every information asset would have an owner (a person).
107.	SAIS	**8.2** Protection	Clarity is required in respect of why this section only covers "information assets" and does not include "IT assets". Suggested changes are indicated below. 8.2.2 Identity and access management: A financial institution must – (a) ensure that access to IT assets, information assets and associated facilities is limited to users, processes, and devices authorised by the financial institution;	See response to comment 105 above. With regard to the change on paragraph (f), the Authorities are of the view that it should remain IT environment.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			(b) ensure that access to IT assets, information assets and associated facilities is managed commensurate with the assessed risk of unauthorised access; (c) establish identity management and access control mechanisms to provide effective and consistent user administration, accountability and authentication; (d) establish security and access control policies and procedures; (e) ensure remote access to IT assets and information assets is only allowed from devices or connections that have been secured according to the financial institution's security standards; and (f) ensure that strong authentication is implemented for users performing remote access to safeguard against unauthorised access to the financial institution's IT ~~environment~~ systems.	
108.	Assupol	8.2	8.2.1 Note the expansion of impact events. This does not affect how Assupol deploys its protection capabilities and practices. 8.2.3 Note the expanded scope contained herein. This does not affect how Assupol will respond to the proposed standard. 8.2.5 Note the amendment for the timing of the review to include at least annually. This does not affect Assupol's policy review regime.	Noted.
109.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.2	Consider adding requirement to ensure financial institutions: 1. Adhere to the least privileged principle 2. Implement user access governance (run annual access certification campaigns) 3. Stipulate Privilege access management controls 4. Stipulate IAM controls for third parties/contractors that engage the institution	Least privileged principle and user access governance have been covered in the Joint Standard. The Authorities are, however, not going into too much detail because of the varying nature of financial

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			5. Develop IAM policies, or standards and procedures at a minimum to guide IAM/PAM/UAG in the institution	institutions covered in this Standard.
110.	BASA	8.2.2 (e) ensure remote access to information assets is only allowed from devices or connections that have been secured according to the financial institution's security standards; and	This may pose a concern for most financial institutions in particular around staff personal mobile devices accessing bank info as well as vendors/3rd parties that connect over VPN to us. However, the term according to the financial institutions security standards then allows leeway with this point.	Noted. Each device that should access your network should be configured with the minimum security standards of the financial institution.
111.	FirstRand	8.2.2 (e) ensure remote access to information assets is only allowed from devices or connections that have been secured according to the financial institution's security standards; and	This may pose a concern for most financial institutions in particular around staff personal mobile devices accessing bank info as well as vendors/3rd parties that connect over VPN to us. However the term according to the financial institutions security standards then allows leeway with this point.	See response to comment 110 above.
112.	FirstRand	8.2.3	**Unauthorised data access and modification** though wouldn't be addressed via DLP but via Encryption or Access Control mechanisms as required under Clause 8.2.3 (d). We recommend that the paragraph be amended as follows: (a) develop comprehensive data loss prevention policies and adopt measures to detect and prevent ~~**unauthorised access, modification**~~, copying, and/or transmission of its sensitive information ~~**whether in motion, at rest or in use**~~;	The Authorities have added 'unauthorised access to data'. We are of the view that the remainder should not be deleted.
113.	FirstRand	8.2.3	Consider ensuring alignment between clause 8.2.3 of the Joint Standard being Data Security and Condition 7 being Security Safeguards of POPIA. This is to avoid duplication and conflict between the two.	The Authorities are of the view that the requirements in this Joint Standard are not contradicting the security safeguards of POPIA, but

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
				rather complementing the requirements.
114.	BASA	8.2.3 (a) develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, and/or transmission of its sensitive information whether in motion, at rest or in use;	Unauthorised data access and modification though would not be addressed via DLP but via Encryption or Access Control mechanisms as required under Clause 8.2.3 (d). We recommend that the paragraph be amended as follows: (a) develop comprehensive data loss prevention policies and adopt measures to detect and prevent ~~unauthorised access, modification~~, copying, and/or transmission of its sensitive information ~~whether in motion, at rest or in use~~; Consider ensuring alignment between clause 8.2.3 of the Joint Standard being Data Security and Condition 7 being Security Safeguards of POPIA. This is to avoid duplication and conflict between the two.	See response to comment 112 and 113 above.
115.	FIA	8.2.3	The requirement is that the third party must meet the equivalent security protocols. This is very difficult to establish without a widely recognised standard. There are also cost implications with having an assessment conducted to ensure compliance. This will become unaffordable for SME FSP's.	The Authorities are of the view that this is a critical requirement to safeguard financial institutions. Kindly refer to the Statement of need for and the expected impact. Whilst the Authorities acknowledge the cost implication of these requirements, firstly the Joint Standard must be implemented in a proportional manner. Secondly, the Statement of Need does provide regulatory, and relief measures available to financial institutions. Finally, although cost implications is appreciated, similarly the opportunity cost of not implementing these

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
				requirements should be taken into account.
116.	SAIS	**8.2.3** Data security	Financial institutions in South Africa maintain offshore relationships with various platforms in different jurisdictions with legislative regimes that may differ in terms of GDPR and POPIA. There may also be inferred accountability through sharing of client information and in some instances access to transact on said platforms for client accounts. The SAIS requires transparency in respect of how data security will be aligned with international best practices to ensure consistency of the approaches implemented by AUs .	Noted. The Authorities are of the view that the most stringent rules should apply.
117.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.3	1. Data must be discovered and a data inventory (data owner, data description, data sensitivity) must be maintained. 2. Data must be classified accordingly 3. Data protection mechanism commensurate with the classification level must be defined by the Institution 4. An Information handling standard must be crafted How does this standard deal with cloud data?	1. It is covered under data identification and classification. 2. Agreed. See 8.1.1 of the Joint Standard. 3. Agreed. See 8.1.1 of the Joint Standard. 4. Information handling is comprehensively dealt with in POPIA. Cloud data is part of information asset and should be treated the same as data on site.
118.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.3 (a)	Not just policies, bust standards and procedures and possibly processes as well. As these provide detailed guidance.	The Authorities are of the view that policies would prescribe processes, procedures and Standards.
119.	ASISA	8.2.3 (a) & (b)	Paragraph (b) appears to be a duplication of paragraph (a). It is proposed to amend paragraph (a) as follows:	To avoid any duplication and to simplify, the Joint Standard has been amended to provide for policies of its sensitive information and secondly to

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			(a) develop comprehensive data loss prevention policies and adopt **and implement appropriate** measures to detect and prevent **data theft,** unauthorised access, modification, copying, and/or transmission of its sensitive information whether in motion, at rest or in use	implement appropriate measures to prevent and detect unauthorised access to data, modification, copying, transmission as well as data theft in systems and endpoint devices.
120.	SAIA	8.2.3 (c)	This requirement remains onerous. While our expectation is that third-party service providers with whom we share sensitive information, or who has access to the company's sensitive information, must have an acceptable level of cyber security in place (which is assessed at the onboarding of the third-party service provider as well as on a regular ongoing basis), small institutions (such as loss assessors) cannot implement the same security standards as an insurer. The cost of doing business will increase across the insurance industry.	See response to comment 115 above.
121.	Guardrisk	8.2.3 (c)	This requirement remains onerous. While our expectation is that third-party service providers with whom we share sensitive information, or who has access to the company's sensitive information, must have an acceptable level of cyber security in place (which is assessed at the onboarding of the third-party service provider as well as on a regular ongoing basis), small institutions (such as loss assessors) cannot implement the same security standards as an insurer. The cost of doing business will increase across the insurance industry.	See response to comment 115 above.
122.	MMI	8.2.3. (c)	This requirement remains onerous. While our expectation is that third-party service providers with whom we share sensitive information, or who has access to the company's sensitive information, must have an acceptable level of cyber security in place (which is assessed at the onboarding of the third-party service provider as well as on a regular ongoing basis), small institutions (such as loss assessors) cannot implement the same security standards as an insurer. The	See response to comment 115 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			cost of doing business will increase across the insurance industry.	
123.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.3 (c)	This sentence does not read well as it lacks clarity. Consider re-writing to simpler sentences.	The paragraph in the Joint Standard has been amended.
124.	BASA	8.2.3 (d) ensure that sensitive information stored in systems and endpoint devices is encrypted and protected by access control mechanisms commensurate to the risk exposure.	This would mean that any data deemed sensitive needs to be encrypted at rest (e.g., data on a share drive or databases etc. This may pose a challenge in environments that do not use full disk or file / folder level or DB encryption. We recommend changing this to "encrypted OR protected by access control mechanisms"	Noted. The Joint Standard has been amended accordingly. However, the authorities have retained the power to require encryption based on the nature, scale, complexity and risk profile.
125.	FirstRand	8.2.3 (d) ensure that sensitive information stored in systems and endpoint devices is encrypted and protected by access control mechanisms commensurate to the risk exposure.	This would mean that any data deemed sensitive needs to be encrypted at rest (eg data on a share drive or databases etc. This may pose a challenge in our environment that don't use full disk or file / folder level or DB encryption. I would recommend changing this to "*encrypted* **OR** *protected by access control mechanisms"*	See response to comment 124 above.
126.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.3 (d)	Consider editing the sentience to include the below because weaker encryptions schemes can still be applied, and this does not provide adequate protection. ensure that sensitive information stored in systems and endpoint devices is encrypted **with industry best practice encryption schemes** and protected by access control mechanisms commensurate to the risk exposure	Encryption schemes will be assessed by the Authorities during supervision. See response to comment 124 above.
127.	MMI	8.2.3 (d)	This paragraph states that sensitive information stored on systems needs to be encrypted. The definition of sensitive	See response to comment 124 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			information covers almost all information held by financial services companies. This requirement is unnecessarily onerous and will be costly and take extensive work to implement, across financial services environments.	
128.		8.2.3 (d)	This paragraph states that sensitive information stored on systems needs to be encrypted. The definition of sensitive information covers almost all information held by financial services companies. This requirement is unnecessarily onerous and will be costly and take extensive work to implement, across financial services environments.	See response to comment 124 above.
129.	SAIA	8.2.3 (d)	This paragraph states that sensitive information stored on systems needs to be encrypted. The definition of sensitive information covers almost all information held by financial services companies. This requirement is unnecessarily onerous and will be costly and take extensive work to implement, across financial services environments.	See response to comment 124 above.
130.	ASISA	8.2.3 (e)	It is proposed to align the wording with the definitions of "cyber incident "and "data" to read as follows: ensure that only authorised IT systems, endpoint devices and data storage mediums, are used to **process**, **retrieve**, communicate, ~~transfer~~ **transmit**, or store sensitive information	The paragraph has been amended accordingly.
131.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.3 (f)	Consider swapping prevent and detect around to follow the order of events.	The Authorities are of the opinion that prevention should remain before detection.
132.	BASA	8.2.3 (g) ensure that the use of sensitive production information in non-production environments must be	We recommend that the section in bold be changed to "the same controls as production must be in place".	The Authorities are of the view that the control environment within the non-production environment should be as stringent as the

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		restricted. In exceptional situations where production data needs to be used in non-production environments, **adequate processes and safeguards must be in place for the data request and approval must be obtained from senior management**;		production environment and therefore the wording has been amended to reflect this view.
133.	FirstRand	8.2.3 (g) ensure that the use of sensitive production information in non-production environments must be restricted. In exceptional situations where production data needs to be used in non-production environments, **adequate processes and safeguards must be in place for the data request and approval must be obtained from senior management;**	Recommendation is that the section in bold be changed to "the same controls as production must be in place".	See response to comment 132 above.
134.	BASA	8.2.3 (j) have an agreement in place for the secure return or transfer of data in instances where the contract, including a	This may not be feasible to enforce on third party vendors / service providers. The initial point on permanent deletion is sufficient. It is impractical to expect the service provider to destroy the storage media as well.	The Authorities are not in agreement with this proposal. It is unclear why this would be impractical. These are matters that can and should be regulated through the

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		contract with a third-party service provider, is terminated and data must be returned. If return is impossible, there must also be processes in place for the permanent deletion of copies of the financial institution's information as well as the secure destruction of storage media containing the financial institution's information;		contractual agreement with the service provider.
135.	FirstRand	8.2.3 (j) have an agreement in place for the secure return or transfer of data in instances where the contract, including a contract with a third-party service provider, is terminated and data must be returned. If return is impossible, there must also be processes in place for the permanent deletion of copies of the financial institution's information as well as the secure destruction of storage media containing the	This may not be feasible to enforce on third party vendors / service providers. The initial point on permanent deletion is sufficient. It will be very impractical to expect the service provider to destroy the storage media as well.	See response to comment 134 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		financial institution's information;		
136.	**Standard Bank**	**8.2.3 (j) Data Security** "If return is impossible, there must also be processes in place for the permanent deletion of copies of the financial institution's information as well as the secure destruction of storage media containing the financial institution's information"	The statement suggests that if returning of data is possible then the vendor does not need to destroy copies of the bank's data. We proposed that the statement should include that *"even if the return of data is possible the vendor is still required to destroy any copies of the data"*. We proposed that the clause should read as follows: *"There must also be processes in place for the permanent deletion of all copies of the financial institution's information as well as the secure destruction of storage media containing the financial institution's information"*	Noted and agreed. The Joint Standard has been amended to reflect this.
137.	Brolink	8.2.3(j)	From the perspective of an intermediary dealing with many different insurers, one may not be able to completely meet the requirement "for the permanent deletion of copies of the financial institution's information". An intermediary must retain certain records in line with statutory retention periods (e.g. FAIS, FICA, Companies Act). Unstructured data such as emails and voice logs cannot necessarily be identified systematically as belonging to one insurer or another. Emails may be held in archival systems to meet FAIS retention requirements but deletion of individual emails from archival systems is not practical. A database of insurance policies, claims and accounting transactions needs to be backed up in totality and one cannot selectively remove records from a historical backup for one insurer but not another. We propose the following insertion: "To the extent that permanent deletion is not practical, a third-party service provider must continue to apply data security controls for as long as the third-party service provider holds data of the financial institution."	Noted. The Joint Standard has been amended to reflect such situation.
138.	Marsh	Section 8: Cyber security and Cyber	Not only users, but vendors and cloud service providers.	A definition of 'user' is in the Joint Standard and would

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		resilience fundamentals bullet point 8.2.3 (k)		include vendors and cloud service providers.
139.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.4	1. Consider adding in requirements for on-going vulnerability scanning and/or ongoing pen tests for existing applications in the landscape. (Not only on change to applications as is stated in (d)). 2. Consider adding controls for protection of application's transactions? 3. Consider adding controls for securing outsourced application development? 4. Consider adding controls for the setup of secure development environments?	1. Sections 8.6.2 and 8.6.3 makes provision for regular vulnerability assessment penetration testing requirements which will apply to application assessments. 2 and 3: The Authorities are of the view that additional security controls will be based on the criticality and sensitivity of applications. 4. This requirement is too granular for the purposes of this Standard. The Authorities may issue Guidance Notices if deemed necessary.
140.	SAIS	**8.2.4** Application and system security	Suggested changes are indicated below. 8.2.4 (b) determine the acceptable level of security required to meet its business needs and assess the potential threats and risks related to the IT system and information assets; (d) ensure that changes to business-critical applications are reviewed and tested to ensure that there ~~are~~ is no adverse impact on operations or security.	Noted. (b) has been amended to refer to 'applications and system'. (d) has been amended accordingly.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
141.	ASISA	8.2.4 (c)	Due to different functionalities of security systems and various means of implementation, it may not be viable for the security requirements to be specified before development or acquisition or during implementation. It is proposed to add the following wording at the end, after the words *"development/acquisition"*: ***"Where the security requirements cannot be specified/implemented, a financial institution shall ensure that compensating controls are implemented;" and …***	The Authorities are not in support of this amendment. The institution is expected to know the minimum security requirements based on criticality and sensitivity of information assets. Furthermore, this Standard also provide for some direction in this regard.
142.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.5	Consider adding in requirements for cloud network connectivity (e.g. point to point vpn's, CSP dedicated connectivity (Azure Express route, AWS Direct connect etc).	This requirement is too granular for the purposes of this Standard. The Authorities may issue Guidance Notices if deemed necessary.
143.	SAIA	8.2.5 Network security A financial institution must – (a) install network security devices to secure the network between the financial institution and the internet, as well as connections with third-party service providers; (b) deploy network intrusion detection or prevention systems to	Clarity is sought as to whether the standard will incorporate cloud computing requirements as most organizations are moving to Cloud.	A Directive and Guidance Note have been issued to Banks on cloud computing. The Authorities will in due course publish, for consultation, a Joint Standard on cloud computing which will apply to the insurance sector as well. However, the principles and requirements captured in this standard in so far as cybersecurity and cyber resilience will apply to relationships with third-party service providers, including cloud computing service providers.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		detect and block malicious traffic; (c) review its network architecture, including the network security design; as well as systems and network interconnections on a periodic basis to identify potential vulnerabilities; (d) implement network access controls to detect and prevent unauthorised devices from connecting to its network. Network access mechanisms must be reviewed regularly, but at least annually, to ensure they are kept up-to-date; (e) review firewall rules on a periodic basis and test network perimeter controls and posture at least annually. (f) isolate internet web browsing activities from its sensitive IT systems through the use of physical or logical segregation, or implement equivalent controls, to reduce exposure of its IT		

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		systems to cyber-attacks; and (g) encrypt remote connections to prevent data leakages through network sniffing and eavesdropping		
144.	FirstRand	8.2.6. Cryptography	There is currently no definition for “Cryptography”. The previous comments do not address this issue, therefore a definition for “cryptography” should be inserted in the Joint Standard.	Noted. A definition has been added for ‘cryptography’ in the Joint Standard.
145.	BASA	8.2.6. Cryptography	The reference to crypto/encryption states that stored sensitive data must be encrypted and all network connections for data transfer must be encrypted. Is the encryption of all sensitive data stored using Transport Layer Security across connections mandatory? There is currently no definition for “Cryptography”. The previous comments do not address this issue, therefore a definition for “cryptography” should be inserted in the Joint Standard.	The PA does not prescribe specific cryptographic methodologies. Refer to the response to comment 123 regarding encryption of sensitive information. Refer to response to comment 144 regarding the definition for ‘cryptography’.
146.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.6	Consider including: Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Please refer to paragraph 8.2.5(g) of the Joint Standard which deals with this requirement.
147.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.2.7	No comment	Noted.
148.	Assupol	8.3	8.3.1 Note the amendment from recognize or detect to monitor and detect. Note the further distinction of monitor and	Noted.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			analysis of cyber events, and detect and respond to cyber incidents. Note further the reduced effectiveness evaluation mechanisms. This however will not affect how Assupol deploys its detection capabilities.	
149.	SAIS	**8.3** Detection	Suggested changes are indicated below: 8.3.1 A financial institution must maintain effective cyber resilience capabilities to – (a) systemically monitor and detect ~~actual or attempted attacks on IT system~~ cyber events and cyber incidents and business services as well as effectively respond to attacks; There should also be an amendment to include the use of the definition as defined in the Joint Standard.	Noted and amended accordingly.
150.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.3.1 (a)	Does this also refer to cloud computing as well?	Yes.
151.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.3.2 (a)	Consider inserting the items in yellow “Establishing a process to collect, review and retain IT system logs to facilitate security monitoring operations. These logs must be protected against unauthorised access, unauthorised editing and deletion”;	Noted and amended accordingly.
152.	Assupol	8.4	No comment	Noted.
153.	SAIS	**8.4.1** A financial institution must	Suggested changes are indicated below: 8.4.1 A financial institution must – (b) establish effective cyber incident management policies and processes that will help to improve resilience, support business continuity,	Noted and amended accordingly.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			improve customer and stakeholder confidence and potentially reduce any impact; There should also be an amendment to include the use of the definition as defined in the Joint Standard.	
154.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.4.1 (d)	Cloud storage implies the potential movement of data outside of SA borders, should this standard provide guidance on the impact of privacy regulation (PoPIA) as backups could contain PII.	Financial institutions are still required to follow the principles and requirements as outlined in POPIA.
155.	ENS	8.4.1(e)	We note the treating customers fairly considerations raised in your response at comment 175 to our earlier comment and are in agreement with this. However, we remain unsure as to what the minimum requirement for a financial institution is. Will it, for example, meet this requirement if a financial institution, within a reasonable period of a cyber-attack, informs its customers that it has been the victim of such an attack, which may have an impact on customers? Please clarify the requirement to indicate to customers any recourse which they may have. This may not be known at the time of the cyber-attack (there may be an internal investigation required to determine fault or negligence) and so a financial institution would, in our view, not be in a position to comply with this aspect of the notification requirement.	It is beyond the scope of this Standard to provide the level of detail in respect of a communication strategy in the event of a cyber-attack. The Authorities may possibly supplement the Standard with a Guidance to provide more detail in this regard. Similarly, to reporting requirement where the Standard provides that these will be determined separately, the Authorities may adopt a similar approach in respect of communication strategies.
156.	BASA	8.4.1(e) Response and recovery A financial institution must implement a clear communication strategy to financial customers impacted by cyber-attacks including details on any	We recommend that the communication strategy be enhanced to outline the minimum period within which a financial institution ought to notify its financial customers of a cyberattack. It would be good conduct to ensure that there are no unnecessary delays in communicating with financial customers about a cyber-attack taking into consideration the impact that such an event can have on them. Of course, this	Agree, with comments. However, at this stage our view is that the detail and time periods in respect of a communication strategy in the event of a cyber-attack, should not be dealt with in this Standard. Possibly the Authorities may supplement the Standard with a Guidance

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		recourse available to financial customers.	would need to be balanced with the necessary risks to the financial institution, which need to be addressed.	to provide more detail in this regard.
157.	FirstRand	8.4.1(e) Response and recovery A financial institution must implement a clear communication strategy to financial customers impacted by cyber-attacks including details on any recourse available to financial customers.	Recommend that the communication strategy be enhanced to outline the minimum period within which a financial institution ought to notify its financial customers of a cyber-attack. It would be good conduct to ensure that there are no unnecessary delays in communicating with financial customers about a cyber-attack taking into consideration the impact that such an event can have on them. Of course, this would need to be balanced with the necessary risks to the financial institution, which need to be addressed.	See response to comment 156 above.
158.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.4.2	Consider removing the word “latest” in the sentence, it is not required to include this as all threats should be covered, not just the latest threats. ensure that the cyber incident response and management plan is tested to address ~~the latest~~ cyber threats.	Noted and amended accordingly.
159.	Assupol	8.5	No comment	Noted
160.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.5.1	No comment	Noted
161.	SAIS	**8.5.2** Threat intelligence and information sharing	Suggested changes are indicated below: 8.5.2 (c) participate in cyber threat information-sharing arrangements with trusted external parties to - (i) share reliable, actionable cybersecurity information regarding threats, vulnerabilities <u>and cyber</u> incidents to enhance defences;	The Authorities are of the view that the root paragraph is narrowing the focus to cyber.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			There should also be an amendment to include the use of the definition as defined in the Joint Standard.	
162.	ASISA	8.5.2 (a)	It is proposed to insert the word ***"to"*** after *"relevance"* and the word ***"on"*** after *"impact"* to read as follows: …for its relevance **to**, and potential impact ~~to~~ **on** the business and IT …	Noted and amended accordingly.
163.	ASISA	8.5.2 (c) (i)	It is proposed to insert the word ***"and"*** after *"vulnerabilities"* to read as follows: ….. vulnerabilities **and** incidents to enhance defences; and	Noted and amended accordingly.
164.	Assupol	8.6	8.6.3 Note the relaxed regulatory powers from direction to discretion to accommodate organizations and treatment on their own terms. Further note the requirement to amending the frequency of the penetration tests. This does not affect how Assupol currently conducts its penetration test strategy. 8.6.5 Note the requirement to frequency of reviewing policies and procedures. This does not affect Assupol's policy review regime. 8.6.6 Note requirement to prioritize issues based on risk posed. This does not affect Assupol's risk management framework. Further note requirement related to known issues. This does not affect how Assupol responds to realized risks.	Noted.
165.	SAIS	**8.6.1** Testing control effectiveness	Suggested changes are indicated below: 8.6.1 (a) (iii) the consequences of a ~~security~~ cyber incident; There should also be an amendment to include the use of the definition as defined in the Joint Standard.	(a) Noted and amended accordingly. The Authorities are of the view that the definition of information assets will include IT assets.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			(b) Where a financial institution's IT assets, information assets are managed by a third- party service provider, and a financial institution is reliant on that party's information security control testing, the financial institution must be satisfied that the nature and frequency of testing of controls in respect of those IT assets and information assets is commensurate with items (a)(i) to (v).	
166.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.6.1 (a) (i)	"the rate at which the vulnerabilities and threats change;" This statement is very broad as the rate at which vulnerabilities and threats evolve is daily, if not hourly. Does the minimum control instead need to specify a required minimum testing frequency (e.g. once a quarter, or monthly?)	The Authorities are of the view that it is not necessary to specify the frequency as it is commensurate to the factors identified in paragraph 8.6.1(a).
167.	ENS	8.6.1 (b)	Consider requiring a financial institution to contractually require third party service providers to perform information security control testing to meet that financial institution's assessment of nature and frequency. Is the intention that any such service provider would be a supervised entity as they are party to an outsourcing arrangement (as contemplated in the Financial Sector Regulation Act)?	By requiring the financial institution to ensure that the third party service provider conduct this testing according to the requirements of this Standard, the Standard places an obligation on the financial institution to consider its relationship with the service provider, whether it results in contractual arrangements or not. The FSR Act defines a supervised entity to include a person with whom a licensed financial institution has entered into an outsourcing arrangement. Considering the definition of an outsourcing arrangement in the FSR Act, the provision of the

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023				
No.	**Commentator**	**Paragraph**	**Comment**	**Response**
				management of information assets is considered to be an outsourced function. The Authorities therefore, have the ability to apply Chapter 9 of the FSR Act with respect to information gathering, inspections and investigations. Outsourcing arrangements have a variable degree of materiality and the robustness of a bank's management of outsourcing risk, must be in line with the materiality of the outsourcing arrangement. Core banking IT systems as well as a bank's financial reporting IT systems are viewed as material business functions. Comprehensive risk assessments such as the specific arrangements underlying the services offered, the service provider, the criticality and sensitivity of IT systems and information assets, vulnerabilities and threats should be periodically undertaken in line with bank's risk management. Banks should identify, assess, manage, mitigate and report on risks associated with outsourcing to meet its

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
				obligations. An outsourcing risk management programme should address risk assessments, ongoing monitoring of service providers, testing of controls in respect of IT systems or information assets, business continuity and contingency planning.
168.	SAIS	**8.6.2** Vulnerability assessment	Suggested changes are indicated below: 8.6.2 Vulnerability assessment A financial institution must – (a) establish a process to conduct regular vulnerability assessments on its IT systems and information assets to identify security vulnerabilities and ensure that vulnerabilities are addressed in a timely manner; and (b) ensure that the frequency of vulnerability assessments is commensurate with the criticality of the IT system and information assets and the security risk to which it is exposed.	Noted and amended accordingly.
169.	SAIA	8.6.2 Vulnerability Management A financial institution must – (a) establish a process to conduct regular vulnerability assessments on its IT systems to identify security vulnerabilities	*Proposed additional point 8.6.2 (c):* All internet facing high or critical security vulnerabilities that are exploitable, must be resolved within 60 days. Deviation from this requirement, must be supported by a compensating control record with qualified business, operational or technical justification for such deviation. *Proposed additional point 8.6.3 (d):* All internet facing high or critical security vulnerabilities that are exploitable, must be resolved within 60 days. Deviation from this requirement, must be supported by a compensating control record with qualified business, operational or technical justification for such deviation.	Based on the nature, scale and complexity of the financial institutions that are covered in the scope of this Joint Standard, the Authorities are of the view that this requirement is too granular and prescriptive. The Authorities may be able to address this area bilaterally with the financial institution or

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		and ensure that vulnerabilities are addressed in a timely manner; and (b) ensure that the frequency of vulnerability assessments is commensurate with the criticality of the IT system and the security risk to which it is exposed.		through guidance as necessary.
170.	FIA	8.6.2	A vulnerability assessment is unaffordable for an SME. Annual licensing for recognised and reputable software is in the region of R150 000.00 per annum (Qualys). Human resources or a third-party cyber security provider will then be required to conduct the assessment, analyse the results, discuss with management, formulate a plan and then implement. These costs are over and above the software licensing.	Disagree with comments. The Joint Standard, provides proportional implementation of the relevant requirement and same must be assessed in consideration of the nature, size, complexity and risk profile of a financial institution. In this light, an appropriate "vulnerability assessment" and "penetration testing" must be applied, taking into account the size and nature of the financial institution. Smaller institutions can therefore, as relevant, implement vulnerability assessments that are less onerous in nature, and much cheaper to acquire. In addition, when implementing and assessing these requirements, the Authorities

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
				will apply supervisory discretion and possibly light touch regulation, taking into account the type, size, nature and complexity of a financial institution.
171.	FIA	8.6.3	Penetration testing for an FSP is again not affordable for an SME financial institution. The cost for this by a reputable provider is high is not affordable. Again, due to lack of a widely recognised standard (e.g. NIST or ISO 27000 series) finding a provider to conduct an adequate penetration test will be extremely difficult and come at additional cost as the provider will need to review the joint standard and attempt to meet the Joint Standards requirements. All coming at an additional cost and risk of non-compliance.	Disagree with comments. See response to comment 170 above.
172.	MMI	8.6.3	This paragraph requires penetration testing of all IT systems at least annually. This may not be practical for environments with an extensive Internet footprint like most financial services companies in South Africa. This because a full penetration test requires 2 or 3 days of work per system. If a company has for instance 200 systems this will be 400-500 days or work, which is very onerous to deal with. We would suggest that at a minimum all Internet facing systems are subject to operating system and application-level vulnerability scans using automated tools least annually.	Noted. The Joint Standard has been amended for the application to be limited to critical IT systems and information assets.
173.	SAIA	8.6.3 Penetration Testing A financial institution must – (a) carry out penetration testing to obtain an in-depth evaluation of its cybersecurity defences.	*Proposed additional point 8.6.3 (d):* All internet facing high or critical security vulnerabilities that are exploitable, must be resolved within 60 days. Deviation from this requirement, must be supported by a compensating control record with qualified business, operational or technical justification for such deviation.	See response to comment 172 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		The Authorities may, based on the nature, scale, complexity and risk profile of the financial institution specify that a black box, grey box and white box testing or a combination thereof be conducted for IT systems and information assets; (b) ensure that the frequency of penetration testing is determined based on factors such criticality and exposure to cyber risks; and (c) conduct penetration testing to validate the adequacy of the security controls for IT systems and information assets that are directly accessible from the internet, whenever such IT systems and information assets undergo 10.major changes or updates. If no major changes or updates are made, the penetration testing must be conducted at least annually.	This paragraph requires penetration testing of all IT systems at least annually. This may not be practical for environments with an extensive Internet footprint like most financial services companies in South Africa. This because a full penetration test requires 2 or 3 days of work per system. If a company has for instance 200 systems this will be 400-500 days or work, which is very onerous to deal with.	

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
174.	Guardrisk	8.6.3 Penetration testing A financial institution must – (a) carry out penetration testing to obtain an in-depth evaluation of its cybersecurity defences. The Authorities may, based on the nature, scale, complexity and risk profile of the financial institution specify that a black box, grey box and white box testing or a combination thereof be conducted for IT systems and information assets;	This paragraph requires penetration testing of all IT systems at least annually. This may not be practical for environments with an extensive Internet footprint like most financial services companies in South Africa. This because a full penetration test requires 2 or 3 days of work per system. If a company has for instance 200 systems this will be 400-500 days or work, which is very onerous to deal with.	See response to comment 172 above.
175.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.6.3 (a)	Consider including the yellow highlights, as this standard aims to stipulate the minimum controls required. The included yellow highlighted words sets the minimum requirement. “carry out penetration testing to obtain an in-depth evaluation of its cybersecurity defences. The Authorities may, based on the nature, scale, complexity and risk profile of the financial institution specify that a black box, grey box and white box testing or a combination thereof be conducted for High Risk IT systems and information assets;”	See response to comment 172 above.
176.	ASISA	8.6.3 (b)	It is proposed to insert the word ***“as”*** after *“such”* to read as follows:	Noted and amended accordingly.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			… based on factors such **as** criticality and exposure ….	
177.	**Standard Bank**	**8.6.3 (c) Penetration Testing** "conduct penetration testing to validate the adequacy of the security controls for IT systems and information assets that are directly accessible from the internet, whenever such IT systems and information assets undergo major changes or updates. If no major changes or updates are made, the penetration testing must be conducted at least annually"	There is a need to investigate the practicality of conducting an annual testing mainly for larger organisations. To address this requirement currently there are other mitigating controls in place for web presence such continuous web scanning and perimeter security scoring capabilities that minimize the risk. It is noted that these practises are not covered in the definition of "penetration testing". We proposed linking the frequency to 8.6.1a or updating to: ` *"conduct penetration testing to validate the adequacy of the security controls for IT systems and information assets that are directly accessible from the internet, whenever such IT systems and information assets undergo major changes or updates. If no major changes or updates are made, the penetration testing must be conducted at least annually, based on risk and criticality"*	See response to comment 172 above.
178.	**Marsh**	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.6.4	Should the minimum control list also prescribe a control for making changes to or updates of the cyber incident response procedure, standard if the simulations have show serious flaws or shortcomings?	Noted, however, the Joint Standard does have requirements relating learning and evolving which will cover this requirement. See paragraph 8.7.
179.	Outsurance	8.6.5	The change in the draft standard is not in line with the agreed changes in the comment matrix. The use and update of as noted in comment 219 has not been inserted into 8.6.5(c)	Noted and amended accordingly.
180.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.6.5 (a)	Consider including the yellow highlights, as continuous testing must be catered for those organisations that employ the DevSecOps model. This requires continuous testing	The Standard has been amended to include development for the purposes of clarity, however, this

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			during the development cycle, and not just during the implementation cycle. " carry out testing of security functionality on web-based and critical applications during the development and implementation in a robust manner to ensure that they satisfy business policies or rules of the financial institution as well as regulatory and legal requirements"	requirement has been covered under the security by design requirements.
181.	ASISA	8.6.5 (c)	It is proposed to delete the ***"s"*** in *"codes"* to read as follows: ….. third party and open-software code~~s~~ to ensure these codes …	Noted and amended accordingly.
182.	BASA	8.6.6. Remediation management (b) (iii) keep track of updates and reported vulnerabilities on third-party and open-source software that are utilised by the financial institutions in order to facilitate the remediation of vulnerabilities in a timely manner.	Where does this need to be reported to?	This is not reporting to the Authorities. It is vulnerabilities reported by third-parties or identified internally within the financial institution.
183.	BASA	8.6.6. Remediation management	What is the consideration for the various product (agile) environments vs the project based environments? Is this standard applicable to both of them or there is a distinction.	Applies to both environments as the same controls are required.
184.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.6.6 (a)	Does the word resolve also include risk acceptance of the issue if a solution is not available or feasible? → If so, consider including reference to risk acceptance of this scenario.	The financial institution must consider this in terms of their risk assessment process and risk appetite. If it within their risk appetite, then it can be accepted. This obviously will

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			"A financial institution must establish a comprehensive remediation process to track and resolve issues identified from the cybersecurity testing or exercises, third-party assessments, self assessments as well as findings from internal and external assurance."	not apply to serious or critical findings in the applications.
185.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.6.6 (b) (ii)	Consider including the yellow highlighted words, as tracking the issue alone does not add too much value or not adequate. The control should include a requirement to address (remediate or risk accept) the issue. "ensure all issues, identified from cybersecurity testing or exercises, as well as software defects discovered from source code review and application security testing, are tracked, remediated or risk accepted."	This sub item must read in totality with the paragraph as it requires that vulnerabilities identified must be resolved. Also see response to comment 184 above.
186.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.6.6 (b) (iii)	Consider including the yellow highlighted words, as in-house developed applications must be subject to this control as well. keep track of updates and reported vulnerabilities on third-party, open-source software, and in-house developed software that are utilised by the financial institutions in order to facilitate the remediation of vulnerabilities in a timely manner.	Noted and amended accordingly.
187.	Assupol	8.7	No comment	Noted.
188.	Marsh	Section 8: Cyber security and Cyber resilience fundamentals bullet point 8.7 (a)	Please elaborate on what the exact requirement is here, is the intention to employ a SOAR type capability? If so, it is recommended that guidance on this be provided, as the statement is broad and allows for an array of interpretations. " implement an adaptive cyber resilience capability that learns and evolves with the dynamic nature of cyber risks and allows the institution to identify, assess and manage	Cyber resilience capabilities includes people, process and systems. Thus all these components must evolve and adapt. If the Authorities deem necessary further guidance may be issued in terms of a guidance notice.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			security threats and vulnerabilities; systematically identify and distil key lessons from cyber events that have occurred within and outside the institution in order to advance resilience capabilities; ” Will this be feasible from a financial perspective for smaller FSI’s ?	Smaller financial institutions will need to apply this requirements in response to their risk profile.
189.	Aurora Insurance	9.Cybersecurity hygiene practices	9.1. Access management – Duly noted. Least privilege access models already applied. 9.2. Privileged access management – Duly noted. 9.3. Multi-factor authentication – Duly noted. 9.4. Network perimeter defence – Duly noted. 9.5. Vulnerability and patch management – Duly noted. 9.6. Secure configurations – Duly noted. Our Change Management framework is being enhanced to incorporate this. 9.7. Malware protection – Duly noted.	Noted.
190.	SAIS	**9.1** Access management	Suggested changes are indicated below: 9.1 (a) establish a security access control policy (which includes identity and access management such as passwords, biometrics, tokens etc.) and a process to enforce strong password security controls for users’ access to IT systems and information assets;	Noted and amended accordingly.
191.	Assupol	9.1	9.1 Note requirement for regular review of policies. This does not affect Assupol’s policy review regime.	Noted.
192.	ASISA	9.1 (a)	It is proposed to delete the wording between brackets to read as follows:	Noted and amended accordingly.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			… control policy ~~(which includes identity ……. biometric, tokens etc)~~ and a process to ……	
193.	ASISA	9.1 (e)	It is proposed to insert ***"s"*** after the word *"review"* to read as follows: …. periodic user access review**s** to verify the ……	Noted and amended accordingly.
194.	Assupol	9.2	No comment	Noted.
195.	BASA	9.2 Privileged access management A financial institution must – (a) ensure that every administrative account in respect of any operating system, database, application, security appliance, network device, cloud tenant or authentication system is secured to prevent any unauthorised access to or use of such account; (b) grant access to privileged accounts on a need-to-use basis; activities of these accounts must be logged and reviewed as part of the financial	Reference is made in Clause 9.2 to "privileged access management" and to"privileged accounts", however, these terms are not defined in the Draft Standard. □ It is not clear what would be regarded as "privileged accounts" or "privileged access management" and we suggest that the Authorities provide more clarity and/or a definition in relation hereto.	Noted. Privileged accounts and privileged user have been defined. The Authorities are of the view that the concept of privileged access management does not need to be defined.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		institution's ongoing monitoring; and (c) establish a process to manage and monitor the use of IT systems and service accounts for suspicious or unauthorised activities.		
196.	FirstRand	9.2 **Privileged access** management A financial institution must – (a) ensure that every administrative account in respect of any operating system, database, application, security appliance, network device, cloud tenant or authentication system is secured to prevent any unauthorised access to or use of such account; (b) **grant access to privileged accounts** on a need-to-use basis; activities of these accounts must be logged and reviewed as part of the financial institution's ongoing monitoring; and (c) establish a process to manage and monitor the use of IT systems	• Reference is made in Clause 9.2 to "privileged access management" and to "privileged accounts", however, these terms are not defined in the Draft Standard. • It is not clear what would be regarded as "privileged accounts" or "privileged access management" and we suggest that the Authorities provide more clarity and/or a definition in relation hereto.	See response to comment 195 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		and service accounts for suspicious or unauthorised activities.		
197.	Assupol	9.3	No comment	Noted
198.	Marsh	Section 9: Cybersecurity hygiene practices 9.3	Consider including MFA requirements for users that require remote access to the corporate network and corporate applications.	This applies to all types of access to critical applications/systems.
199.	ASISA	9.3 (a) & (b)	It is believed that (a) is covered by (b) and it is therefore proposed that (a) could be excluded.	The Authorities are of the view that (a) and (b) refer to different concepts.
200.	MMI	9.3 (a)	This paragraph requires MFA on "critical system functions". Please include a definition for "critical system functions".	Please see definition of criticality and financial institutions must be able to identify their own critical systems. What is critical to one financial institution may not be critical to another.
201.	SAIA	9.3 (a)	This paragraph requires MFA on "critical system functions". Please include a definition for "critical system functions"	See response to comment 200 above.
202.	Guardrisk	9.3 (a)	This paragraph requires MFA on "critical system functions". Please include a definition for "critical system functions"	Please see response to comment 200.
203.	SAIA	9.3 (b)	This paragraph that requires MFA on all administrative and privileged accounts is very onerous and will be hard to implement across all environments on an application, database, operating system level in a reasonable timeframe. We would suggest applying MFA to privileged accounts on Internet facing systems.	The Authorities are of the view that this proposal does not address internal threats and only captures certain users. Financial institutions will be given adequate time to implement this requirement.
204.	Guardrisk	9.3 (b)	This paragraph that requires MFA on all administrative and privileged accounts is very onerous and will be hard to implement across all environments on an application, database, operating system level in a reasonable timeframe. We would suggest applying MFA to privileged accounts on Internet facing systems.	See response to comment 203 below.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
205.	MMI	9.3 (b)	This paragraph that requires MFA on all administrative and privileged accounts is very onerous and will be hard to implement across all environments on an application, database, operating system level in a reasonable timeframe. We would suggest applying MFA to privileged accounts on Internet facing systems.	See response to comment 203 above.
206.	FirstRand	9.3 (b) ensure that MFA is implemented for all administrative and privileged accounts;	It may also not be feasible for all administrative accounts on every system, particularly if a system cannot integrate into MFA/2FA tools. For example local windows or local linux local admin accounts or built in admin accounts in various systems. It would be better if the clause rather stated that a Privileged Access Management mechanism/tool should be in used.	Noted and amended to include 'at least privileged access management mechanisms'.
207.	BASA	9.3 (b) ensure that MFA is implemented for all administrative and privileged accounts;	It may not be feasible for all administrative accounts on every system, particularly if a system cannot integrate into MFA/2FA tools. For example, local windows or local linux local admin accounts or built in admin accounts in various systems. It would be better if the clause rather stated that a Privileged Access Management mechanism/tool should be in used.	See response to comment 206 above.
208.	Assupol	9.4	No comment	Noted.
209.	SAIA	9.4 Vulnerability Assessments	The current definition of "vulnerability assessment" is inconsistent with the generally accepted definition and may be confused with a "risk assessment". This is because a "risk assessment" includes "a systematic review of controls and processes", this is not done in a vulnerability assessment, which usually just looks for vulnerabilities in a system. We would recommend using the NIST definition: "Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation."	See response to comment 15 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
210.	Assupol	9.5	No comment	Noted.
211.	Marsh	Section 9: Cybersecurity hygiene practices 9.5 (b)	Consider adding in the yellow highlighted word just for completeness purposes. "Compensating security controls are instituted to reduce any risk posed where there is no security patch available to address vulnerabilities identified;"	Noted and amended accordingly.
212.	**Standard Bank**	**9.5 (c) Vulnerability and patch management** "security patches are tested before they are applied to the IT systems in the production environment to ensure compatibility with existing IT systems or such patches do not introduce problems to the IT environment."	For instances where patches are not complaint with the running of the IT system or impact the stability of the IT environment, there needs to be commentary on the minimum mitigating requirements. We propose link to 8.6.1(c) iii: *"(d) where patches are not compatible with existing IT systems or such patches introduce problems to the IT environment, ensure that a remediation plan, with timelines is followed to address identified control deficiencies."*	Noted and amended accordingly.
213.	ASISA	9.5 (c)	It is not always practical in all instances for security patches to be tested prior to it being applied to the IT system. It is proposed to add the following wording at the end after the words *"… to the IT environment"*: ***"Where the institution is unable to test all security patches to be deployed, the financial institution shall ensure that, adequate compensating controls are implemented, to sufficiently remediate any negative impact on the IT environment***".	The Authorities are of the view that it would be difficult to ensure adequate compensating controls if the financial institution has not tested the security patches and understood its impact on systems and the IT environment.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
214.	Marsh	Section 9: Cybersecurity hygiene practices 9.6	Would it be prudent for the standard to stipulate a requirement for “golden images” to be created maintained and applied?	The Authorities are of the view that the proposal introduces granularity in the requirement which may not be feasible for all the financial institutions that are covered in the scope of the Joint Standard.
215.	Assupol	9.6	No comment	Noted.
216.	Assupol	9.7	No comment	Noted.
217.	Aurora Insurance	10 Notifications and regulatory reporting	Duly noted. We are monitoring developments closely.	Noted.
218.	Assupol	10	No comment	Noted.
219.	ENS	10.1	Please clarify whether the financial institution may in their discretion (and in accordance with their framework) determine whether an incident is material. Financial Institutions will need assurance that their determination, as long as it is in line with their policies, will stand and that they could not be found in contravention of this requirement if the Authorities disagreed with the determination (for example believed that an “immaterial” incident should actually have been reported as a material incident).	Please see definition of material incident.
220.	SAIA	10.1	Point 10 discusses the requirements of reporting to an authority (PA or FSCA). Our assumption is that we (as an insurer) would always be reporting to the Prudential Authority (and, where applicable, the Information Regulator, although we are of the view that this is outside the scope of this standard). It is however unclear whether we are also obliged to report to the FSCA. From the notification template it appears as if we will also have to notify the FSCA, however clarity is sought in this regard.	Reporting must be done to the responsible authority – please see definition of responsible authority which has been inserted.
221.	Aurora Insurance	11 Short title	Duly noted.	Noted.
222.	Assupol	11	No comment	Noted.
223.	Aurora Insurance	Material IT and/or cyber and information security	Duly noted.	Noted.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		incidents report form (cover page)		
224.	Aurora Insurance	Material IT and/or cyber incidents report form (contact details)	Duly noted.	Noted.
225.	Aurora Insurance	Material IT and/or cyber incidents report form (details of the incident)	Duly noted. We don't understand the need to report a preliminary incident classification being "Incident occurred on non-critical system". In our classification system this is not a 'code red'.	Noted.
226.	Aurora Insurance	Material cyber incidents report form (information of a cyber incident)	Duly noted.	Noted.
227.	Aurora Insurance	Root cause and impact analysis report (impact of the incident)	Duly noted. We suggest that a grading system be added to determine a 'threshold' for reporting to the Authorities. Most incidents affect non-critical systems or the impact on a critical system may not be severe enough to alert authorities. With a grading system, an agreed threshold needs to be triggered to warrant alert.	Noted.
228.	ASISA	**TAB: Information and Cyber Incident** Lines 11-15	Consider aligning with the incident categories already in use in ASISA and SABRIC. Under malware - SQL injection doesn't fit as it is usually used when hacking poorly configured websites.	The authorities may possibly consider ASISA/SABRIC's categorisation in future. The incident reporting template is applicable to small and large institutions, and the Authorities are of the view that it is still relevant.
229.	ASISA	Line 16	Information Related to attackers - Should probably not be a selection filed but rather freeform text field.	Noted. Information related to attackers has been changed to category of attacker. The dropdown has been adjusted accordingly.
230.	ASISA	Line 18	Vulnerabilities and Weaknesses exposed – often the incident exploits a combination of multiple weaknesses like poor configuration, poor logical access controls and poor network	Noted, to be incorporated/updated accordingly

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			configuration controls. The drop down forces the selection of only one. It is proposed to allow the choice of multiple, as valuable information might be lost.	
231.	ASISA	**TAB: Impact of the incident** Line 22	Media coverage should include social media coverage as well.	Noted
232.	ASISA	Line 40	It should be more specific. What does rectify mean? Containment of the attack, recovery of impacted services, full restoration of capacity or implementing measures to restrict re-occurrence?	Rectify refers to the end-to-end process which includes concepts of identification, containment of the attack, recovery of impacted services, full restoration of capacity or implementing measures.
233.	WTW (Willis Towers Watson)	Cover Page – "When to submit / What to submit"	It is clear that a "material incident" affecting a systemically important financial institution will very likely give rise to "material incidents" at many other financial institutions to which the systemically important institution provides services. Consider for example an incident leading to a bank, insurer, or large pension fund administrator having to declare force majeure for a period and suspend its services to other financial institutions (e.g. pension funds) that are its clients – this would surely result in "material incidents" as defined, for all these client institutions. The Authorities must just be aware that all the client institutions will then also be required to submit notifications - which will potentially result in a very large number of notifications, essentially arising from the same incident. (Of course, this may fit in with the Authorities' requirements, e.g. to understand the systemic "ripple effects" that a material incident at a systemically important institution may have.) "24 hours following discovery" may be a bit ambitious for the client institutions (who will be dependent on their service provider both to disclose the incident and to provide details),	It is 24 hours after categorising the incident as material.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			although we note that the information to be disclosed within the first 24 hours is quite limited. (Note that we are not objecting to the process here – we are just pointing out the implications.)	
234.	Assupol	General	Assupol is in alignment with the template and we commit to compliance with its provisions	Noted.
235.	SAIA	Annexure D Material cybers and IT incidents reporting template. General comments	The reporting template seems to now include reporting of IT incidents. It is essential to note that there are IT standards which deal with IT incidents as well as privacy incident reporting requirements. The regulatory requirement may potentially overlap. Was this the regulators intention? How will the regulator deal with this? It is recommended that reference to IT incidents be removed.	No, we are currently utilising a joint form for both IT and cyber incidents. An IT form or cyber form will be completed based on the type of incident reported.
236.	SAIA	Annexure D Material cybers and IT incidents reporting template. Contact details	Notification to PA and/or FSCA – clarity is required as to the submission process and portal that will be used to submit this information to avoid duplication. Name of institution – It is noted that the template will be used by a number of financial institutions. Fields can be automated and aligned to other PA report templates to avoid numerous naming conventions or errors. Name of person – insert a declaration confirming the completeness and accuracy of the information submitted. c clarity is required as to whether the regulator require a specific person/role to sign off the report.	The notification must be sent to the responsible authority of the financial sector law in terms of which the financial institution is licensed. Noted and will be updated accordingly. The Authorities do not prescribe; however, an individual must be authorised to sign off the form. Declaration has been inserted.
237.	SAIA	Annexure D	Drop downs – please provide terminology for the terms used.	Terminology has been updated.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
		Material cybers and IT incidents reporting template Details of incident, information of a cyber incident, impact of incident	"impact of incident" – there are instances where some of the information required may not be available when the material cyber incident must be reported.	Institutions are required to submit form B after 14 days of reporting the incident.
238.	SAIA	Annexure D Material cybers and IT incidents reporting template. General comments	The reporting template seems to now include reporting of IT incidents. It is essential to note that there are IT standards which deal with IT incidents as well as privacy incident reporting requirements. The regulatory requirement may potentially overlap. Was this the regulators intention? How will the regulator deal with this? It is recommended that reference to IT incidents be removed.	See response to comment 235 above.
239.	Netcash	Whole Standard	We have worked through the draft Joint Standard and believe that the requirements are reasonable to protect the Financial Services Industry and its stakeholders.	Noted.
240.	Guardrisk	General	In recent years, the availability of skilled IT resources within South Africa, with experience in financial services, has reduced due to a number of different reasons. The cost of appointing skilled IT resources across 1st, 2nd and 3rd line in order to implement and comply with the minimum requirements set by the cyber security joint standards will only increase, further driving up the cost of compliance. We urge the joint regulators to carefully consider what should be classified as 'minimum requirements' and welcome the application of the principle of proportionality (in other words, reflect the nature, size, complexity and risk profile of a financial institution) as this principle will need to be applied to comply with the requirements set by the joint standards.	Noted. The Standard contains minimum requirements and if there are any issues in terms of compliance it must be addressed on a bilateral basis with the Authorities.
241.	Guardrisk	Commencement	We urge the joint standards regulators to consider a transitional period of greater than 12 months after the commencement of the joint standard. The joint standard	Based on the criticality of the risk involved, the Authorities are unable to extend this

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			remains onerous and will likely require more than 12 months to fully implement considering all other competing responsibilities. Furthermore, we request a stabilisation period of at least three months post - implementation to ensure implementation was successful.	period beyond a 12-month transitional period.
242.	Aurora Insurance	Joint Standard	We have seen this standard evolve appropriately since it was first proposed. The comments from other institutions indicate a sensitivity to cost-appropriate implementation. Our only concern is the prohibitive cost of an Intrusion Detection System.	See response to comment 240 above.
243.	Aurora Insurance	Material IT and/or cyber incidents report form	The matrix is quite comprehensive, but we suggest a built-in grading system with a 'threshold' that triggers the need to alert the Authorities.	The threshold is the classification of the incident as material.
244.	Grindrod	Whole Standard	Kindly note that Grindrod Bank Limited has no comments to the Joint Communication 4 of 2022 - Notice of invitation for comments.	Noted.
245.	ASISA	5.12 Statement of Need	Consider extending scope of exemption to all financial institutions regardless of size and scale. It is proposed to delete the word ***"small"*** before "*financial institution*" to read as follows: … specific requirement is too onerous on a ~~small~~ financial institution despite the application of the …	Noted. Amendment made to the Statement accordingly.
246.	ASISA	Transitional period	The 12-month transitional period from the date of publication to comply with the proposed Standard is a concern given all what is required to be implemented, the financial impacts, and the probability that additional staff will be required. It is proposed to consider a transitional period of at least 18 months.	See response to comment 241 above.
247.	WTW (Willis Towers Watson)		(We don't have any further comments at this time.)	Noted.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
248.	JSE	Effective date and transition provision	We note that the Revised Joint Standard does not provide for commencement date nor transition provisions. The Statement of the need for, expected impact and intended operation of the proposed Joint Standard (Annexure B), the Authorities provided – *"…To allow ample time for the enhancements of the security controls, the Authorities have provided for a 12-month transitional period following the publication of the Joint Standard. This transitional period would provide the industry with an opportune time to remediate existing gaps and implement necessary enhancements to fully comply with the requirements of the Joint Standard*". We acknowledge that the requirements of revised Joint Standard, once embedded in the risk frameworks of financial institutions, will enhance the security and resilience of the financial markets against cybercrime. However, the frequency of cyber-attacks is increasing, and the methodologies and sophistication of cybercriminals is constantly evolving. In an evolving risk environment, a 12-month transition period is not sufficient time for a financial institution to fully comply with the Joint Standard. We note your response to JSE Group's comment regarding prioritisation of material contracts with third-party service providers: *"Financial institutions will be provided with 12- months within which to implement the Joint Standard and they are free to prioritise which contracts must be amended first."* While we appreciate the recognition of the necessity to prioritise the amendments of contracts, to fully comply with the Joint Standard requires more than the amendment of contracts: Financial institutions are obligated to set up systems, establish governance arrangements and implement	Noted. Where financial institutions are unable to comply within the 12 month period, an application for extension for compliance must be submitted to the responsible authority with a plan on when the financial institution will be able to fully comply with the requirements of the Joint Standard.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			resource-intensive processes to monitor and manage the third-party's compliance with the contractual agreement and the certain requirements in the in the Joint Standard applicable to third-parties. This will require enormous effort, budget and time to implement and to fully comply with the Joint Standard. Consequently, we strongly recommend that a transition period of at least 36 months is provided for in the Joint Standard.	
249.	FIA	Cost restraints and lack of a widely recognised standard	- Lack of a definition of recognised standard (e.g. NIST or ISO 27000 series) means that whether employing human assets in the Cyber Security role OR contracting to a third party. A new "strategy" will need to be researched to meet the needs of this new standard vs. being able to implement an existing proven strategy. This is an evolving space with the threat landscape changing daily but without a reasonable and recognised start point, it will take months of consulting the "Revised Joint Standard – Cybersecurity and Cyber Resilience" to build a suitable framework and this is before implementation and testing. o There is mention of the Revised Joint Standard – Cybersecurity and Cyber Resilience being in line with best practice which is true, but it still lacks enough conformity to align with a widely recognised standard that can be adhered to, to avoid non-compliance and leaves an opening for interpretation and creates a large litigation risk. - This goes further into the cost of employing human assets with the required skill set comes at a very high-cost point due to lack of skills in the market, allowing the contractor or prospective employee to bill high rates. - There are also simply not enough skilled persons or providers to provide these resources to meet the newly required demand. - This is going to force many FSP's to move to international cloud platforms to meet security requirements, thus	Noted. The Joint Standard does align with international best practice. This Joint Standard must then be used as the minimum requirements for cybersecurity and cyber resilience with respect to financial institutions. See response to comment 248 above in terms of application to extend compliance. Due to the serious risk that is posed to financial institutions by cyber risk, the Authorities are of the view that the minimum requirements of this Joint Standard must be implemented by financial institutions to ensure protection and readiness in this evolving environment.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			importing services instead of using local hosting/ software/ hardware providers. Even this will be difficult due to it not being a recognised standard, finding a provider and retrofitting existing platforms to meet the needs of the Revised Joint Standard – Cybersecurity and Cyber Resilience is going to require more time, testing and increase costs. - (Annexure B section 5) Set up costs are referred to on an annual weighted average of 2.9%, this was gathered from only 4 commentators. Smaller FSP's don't have the resources to conduct a study of this nature and the annual weighted average costing would far exceed 2.9%. The basic costs of communications and productivity software for small FSP's may exceed this amount.	
250.	FIA	Timeframe	- A 12-month implementation strategy is not sufficient for the implementation of a comprehensive Cyber Security Strategy that would meet the compliance requirements of the Revised Joint Standard – Cybersecurity and Cyber Resilience - These strategies are usually set over a 2 – 5-year period due the complexity, financial impact, recruitment of persons with the required skill sets, with an annual review to ensure goals are being met and executing remedial action if required. o References: ▪ State of Illinois Cybersecurity Strategy: https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Pages/cybersecurity.aspx ▪ U. S Department of Energy: https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20	See response to comment 248 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			Strategy%202018-2020-Final-FINAL-c2.pdf	
251.	FIA	Requirement for the security controls to be adequate based on an FSP's size, risk appetite, nature, complexity and risk profile.	- This lacks definition and is open to interpretation which leaves room for "unintentional" non-compliance and litigation risk.	Noted. The adequacy will be assessed by the Authorities during supervisory interventions.
252.	FIA	3rd party servicer providers: The Joint Standard does not apply directly to third-party service providers, however where a financial institution is utilising the services of third parties, the security controls of the third-party must be equivalent to that of the financial institution.	How would this be determined? The joint standard is not a widely recognised standard. This there is no way to determine the third parties' level of compliance. Further to this due to lack of skill sets in Cybersecurity within South Africa there are simply not enough qualified persons for the defined financial institutions to employ, thus third-party institutions will need to be used.	Financial institutions contract with third-party service providers and thus the responsibility is with the financial institution to ensure that the security measures implement by the third party are equivalent or similar to that required in term of this Joint Standard.
253.	FIA	The FIA previously requested that a proportional approach be applied here. For smaller Category II FSPs, these requirements are particularly onerous.	The response provided by the Authority requires additional clarity: How are risk appetite, nature, size and complexity of a financial institution defined? What guidance and support will be provided? How will exemptions be applied for? Under what circumstances will exemptions be given?	The nature of the risk management framework for an institution with lower risk is different from the nature of a risk management framework for a highly complex and digital financial institution. Please see response to comment 148 on the applications for extension for compliance.
254.	SAIS	Transitional Period	To ensure that the correct processes and procedures, resources and systems are in place as well as to ensure	Due to the nature of cyber risk, it would not be feasible or responsible to delay the

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			compliance to the Joint Standard, the SAIS requests a transition period of 24 months.	implementation of this Joint Standard longer than 12 months.
255.	SAIS	COFI	The SAIS is cognisant of the fact that with the implementation of COFI, regulation must be streamlined to ensure that the objectives of COFI and other Codes of Conducts and Standards be aligned to ensure that there is regulatory interoperability and thereby making certain that no regulatory arbitrage and duplication of requirements occurs creating unlevel playing fields and possible barriers to entry.	Noted.
256.	SAIS	Costs and Barrier to entry	The SAIS understands that costs and barriers to entry were considered. However, cognisance must be taken of the very definite impact to businesses of all sizes and complexities even if a risk-based approach has been considered and adopted.	Noted. Please refer to the Statement of need for and intended operation and expect impact.
257.	SAIS	Industry Engagement	The SAIS strongly appeals to the FSCA to engage with the Institute *as the Industry Association for Authorised Users (AUs).* The SAIS holds the strong belief that it can provide proactive feedback prior to the drafting of these codes. This will ensure practical application and implementation due to the specialised and niche nature of our understanding of the business of AUs. The SAIS is committed to bettering the South African financial markets and looks forward to a closer and more collaborative working relationship.	Agree with the comments.
258.	Batseta	Statement of Need	**Introduction & Background** Batseta welcomes the publication of the proposed standard on cybersecurity and cyber resilience requirements for financial institutions. The pensions sector covers various permutations with regards to fund operations, amongst these, are some of the following categories: 1. Funds that outsource their administration and/or investments services, commonly referred to self-administered funds;	Noted.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			2. Funds that outsource their administration and/or investments services, commonly referred to professionally administered funds; 3. Funds that are established by a sponsor for commercial purposes, generally insource their administration, investments, and most other services, commonly referred to as umbrella funds. This note deals with funds that fall within the first 2 categories above only. It is common cause that most retirement funds are consumers of broader financial services, and the providers of these services have either been victims of cyber-attacks and/or incidences or remain at cyber risk. **It is noted that all three categories have similar general concerns**: that cybersecurity has become a more dynamic field which is increasingly agile and rapidly adjusting and shifting to keep pace with equally rapid financial services inventiveness as a response to digitization	
259.	Batseta	Statement of Need	**Status quo** This in turn places additional responsibility on retirement funds to ensure that their inhouse and third-party service providers strengthen their ability to anticipate, detect, protect, respond, recover as well as mitigate and adapt to cyber threats in order that they can rapidly recover from cyber incidents and continue to operate with added resilience. **Legal position in respect of duties and information accountability of trustees** We digress at this point to reflect on the duties and responsibilities of retirement fund trustees. In summary, retirement fund trustees are ultimately accountable for the safety and security of fund information, even though they may delegate certain roles and responsibilities to inhouse and/or service providers, they cannot abrogate these responsibilities.	Noted.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			Trustees have a responsibility for IT governance as part of their corporate governance roles. They are accountable for information safety and security at (two)important touch points: a) Where trustees outsource services to third parties, this is where most of the data security breaches arise. In all these instances, the role that trustees need to fulfil is that of ensuring that there are adequate checks and balances in place to ensure that the data is being properly maintained by service providers. b) From time-to-time member data is shared with trustees to assist with decision making on member specific cases – this may be discretionary or non-discretionary. In these instances, the role that trustees need to fulfil is that of ensuring that their own personal cyber hygiene, by virtue of their hardware and software are protected from vulnerabilities. c) Trustees need to ensure that requisite policies and procedures are in place to regulate the environment and mitigate negative events and incidents. ISO 38500 is the international standard that assists organisations of all types and sizes with alignment of organisational decisions with their legal/ regulatory and statutory obligations. King IV proposes policies, frameworks, and standards for technology governance to ensure that inter alia there is appropriate response to cybersecurity risks and that the Board (or governing body) and ensures that it has independent assurance on the effectiveness of cybersecurity strategy for resilience. ISACA (Information Systems Audit and Control Association) also sets general standards to benchmark against.	
260.	Batseta	Statement of Need	**Secure avenues or sites** As consumers of financial services retirement funds utilise communication portals established by the administrator to create the necessary efficiencies in service delivery. Examples of such portals may include a fund (insourced or	Comments noted. See response to comment 63 above.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			outsourced) portal where fund documents such as board packs, fund policies and guidelines, etc could be accessed by the management staff of a fund, principal officer and trustees. Membership portals are also managed by the administrators. Members can access their benefit statements and other relevant information through these secure portals. Employee Benefit Administrators, Consultants, Asset Managers, Actuaries, Auditors, and Lawyers host fund information in various degrees. Similarly, independent principal officers and independent trustees who render a specific service to the fund are provided with or retain fund information or have technological access thereto. Proportional application of the standard on cybersecurity and resilience requirements are thus appropriate especially in relation to the service rendered by principal officers and trustees who do not use sophisticated technology to execute their duties. In most instances principal officers and trustees will use the basic tools of trade such as a computer, printer, and mobile phones. We have some way to go before principal officers and boards of trustees to fully grasp the extent of their responsibilities towards cyber security. The Joint Standard on cybersecurity and resilience is necessary, to raise the level of awareness and highlight roles and responsibilities, as per King IV Principle 12 on Technology and Information governance **Outsourced services** Retirement Funds have little to no control over the outsourced service providers IT operations and the flow of data once it has left the fund, technically speaking where funds are professionally administered, data passes from the employer or other service providers, directly to the fund's s13B administrator, simply bypassing the fund. Realisation by Trustees of their responsibility for corporate governance and by extension IT governance as a part thereof is crucial. Part of the Terms of Conditions of Contract for external service providers or part of the Service Level Agreement for	Agree with comments. Agree with comments. With regards to control over outsourcing of service providers, please note that a financial institution may outsource such functions as it deems necessary. However, a financial institution must ensure that roles and responsibilities are clearly defined in the contract or Service Level Agreement with third-party service providers. Further, notwithstanding any outsourcing of functions, the financial institution remains ultimately accountable for complying with the requirements in this Standard

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			insourced administrator services should very clearly specify what the information security and responsibilities and accountabilities for cybersecurity are. NOTE: There is still no requirement for a fund that only administers its own records to have a license and thus several funds are not administered by a 13B licence holder. Considering cyber security, it might be an appropriate time to address the matter.	
261.	Batseta		Regulators roles and responsibility Consistency in the management of cybersecurity risk through enhanced and standardised cybersecurity requirements are of the utmost importance. It will also inform the supervisory discretion that will apply during compliance assessments. The regulatory framework should therefore provide guidance on what would constitute adequate and robust processes and procedures for managing cyber risks within a retirement fund context. This type of guidance could take the form of a Conduct Standard or Practice Notes. What the Conduct Standard or Practice Notes should provide guidance on Since trustees are not cyber experts, some practical actions that can be taken by trustees and principal officers, under specific guidance of the FSCA and PA and with due regard to codes of good practices, include, amongst others: ▪ Establishment of a robust overall fund information and technology security policy, including cyber security and resilience as one of the primary pillars;	Since this Joint Standard cover a wide scope of financial institutions, the supervisory interventions by the Authorities will place a big role in considering adequacy of the controls and policies put in place by the different financial institutions. It is beyond the scope of this Standard to detail how the requirements will be tested or implemented such as what constitute adequate and robust processes. The Authorities may possibly in due course and supplement the Standard with a Guidance to provide more detail. Such guidance may be a result of detailed assessment of the Standard post implementation.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			▪ Reviewing and enhancing information transfer amongst stakeholders; ▪ Ongoing review of service provider cyber security and resilience standards and controls as part of the Terms and Conditions of Contracts and Service Level Agreements. ▪ Regular compliance testing both internal and outsourced processes and procedures. Furthermore, cyber-attack insurance is prohibitively expensive, considering all these costs associated with compliance. The authority needs to give guidance on what an acceptable expense ratio would ally be helpful to self-administered funds.	
262.	SAIA	Implementation period	The general concern is the timeframe to comply. Twelve months is too short, given all the activities required. Initiatives to comply bear financial impact, and the standard implementation will require additional staff to meet 12 months deadline. Depending on the responses from the Regulators, there may be structural changes to address the Governance section requirements. The joint standard remains onerous and will likely require more than 12 months to fully implement considering all other competing responsibilities. It is therefore recommended that consideration be given to an extended period to comply with all the requirements (a transitional period of 24 months after the commencement of the joint standard). Furthermore, we request a stabilisation period of at least three months post - implementation to ensure implementation was successful.	See response to comment 254.
263.	SAIA		In recent years, the availability of skilled IT resources within South Africa, with experience in financial services, has reduced due to a number of different reasons. The cost of appointing skilled IT resources across 1st, 2nd, and 3rd line in order to implement and comply with the minimum	Noted. Please see Statement of need for, intended operation and expected impact.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
			requirements set by the cyber security joint standards will only increase, further driving up the cost of compliance. We urge the joint regulators to carefully consider what should be classified as 'minimum requirements' and welcome the application of the principle of proportionality (in other words, reflect the nature, size, complexity, and risk profile of a financial institution) as this principle will need to be applied to comply with the requirements set by the joint standards.	
264.	MMI	General	In recent years, the availability of skilled IT resources within South Africa, with experience in financial services, has reduced due to a number of different reasons. The cost of appointing skilled IT resources across 1st, 2nd and 3rd line in order to implement and comply with the minimum requirements set by the cyber security joint standards will only increase, further driving up the cost of compliance. We urge the joint regulators to carefully consider what should be classified as 'minimum requirements' and welcome the application of the principle of proportionality (in other words, reflect the nature, size, complexity and risk profile of a financial institution) as this principle will need to be applied to comply with the requirements set by the joint standards.	See response to comment 263 above.
265.	FirstRand		The Joint Standard requires a Financial Institution to have adequate cybersecurity and cyber resilience measures in place. The proposed Joint Standard sets out the requirements for sound practices and processes of cybersecurity and cyber resilience for financial institutions. Has the provisions of the Cybercrimes Act and the requirements placed on Financial Institutions to identify and report Cybercrimes etc. been considered, so that there is an alignment and a complete overview on the requirements for both the Joint Standard and the Cybercrimes Act incorporated into the adequate cybersecurity and cyber resilience measures that must be in place and prevent a duplication relating to cyber risks?	It is the view of the Authorities that the requirements of this Joint Standard do not contradict the requirements of other legislation.

Table 3 – Full set of comments received during the public consultation conducted in 2022/2023

No.	Commentator	Paragraph	Comment	Response
266.	Moody's		Moody's Corporation ("MCO") would like to thank the Financial Sector Conduct Authority ("FSCA") for the opportunity to comment on the proposed Joint Standard on cybersecurity and cyber resilience requirements ("Joint Standard"). MCO acknowledge the FSCA's initiative to develop regulatory standards for cybersecurity to ensure that organizations have a sufficient level of security in place to protect against cyber threats. MCO also recognises that the Joint Standard is closely aligned with international standards and as a global integrated risk assessment firm, we support this alignment so as to avoid disproportionate regulatory burden or a less effective regime. As the FSCA implements and ultimately takes the Joint Standard into its supervisory toolkit, it is important that the FSCA continues to look to and interpret the Joint Standard alongside the relevant international standards and to recognise that large multinational institutions such as MCO will implement cyber resilience requirements on a global basis, using global resources, policies and procedures.	Noted.

Table 4 – Summary of comments received from the consultation conducted in 2023

Paragraph of the Joint Standard	Summary of comment s	Response from the Authorities
Commencement of the Joint Standard	• Institutions were concerned about the transitional period and indicated that we need to consider giving sometime to enable them to perform a detailed gap analysis of existing controls against the proposed Joint Standard. • Smaller entities may also struggle to meet the compliance deadlines for the Joint Standard.	• It is the view of the Authorities that a 12-month transitional period is adequate for preparation to ensure full compliance with this Joint Standard. • The Joint Standard will be published and from the publication date a 12-month period will be given to financial institutions to implement the requirements of the Joint Standard. • Extensions for compliance will also be considered on a case-by-case basis.
Application of the Joint Standard	• Request for clarity if the standard will be application to third party service provider. • Clarity if the Joint standard only applies to institutions within the South African jurisdiction. • Clarity on how the requirements of the Joint Standard will apply in terms of financial sector laws and prudential/conduct standards, other instruments that deal with similar subject matter, cybersecurity related laws and supersedes internationally recognised security frameworks. • 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.	• The Standard does not apply directly to third-party service providers, however where a financial institution is utilising the services of third parties, the controls of the third-party must be equivalent to that of the institution. • The Joint Standard applies on a consolidated and solo level and must be read together with financial sector laws and instruments issued thereunder. It applies to subsidiaries and branches within and outside the Republic. The Standard applies in addition to the requirements of other pieces of primary legislation. • The best practices were considered in the drafting of the Joint Standard and the requirements should not be contradictory. The minimum requirements and principles of this Joint Standard must be implemented to reflect the nature, size, complexity and risk profile of a financial institution. • The Standard refers to 'appropriate, adequate, effective, and timely' and compliance will be assessed in terms of the nature, complexity, scale, risk profile of the financial institution.
Definitions and interpretation	• Request for clarity on certain terms used in the Joint Standard.	• Clarification was provided on terms. Additional terms were also defined such as cyber event and information security.

Table 4 – Summary of comments received from the consultation conducted in 2023

Paragraph of the Joint Standard	Summary of comment s	Response from the Authorities
		Definitions were also expanded on or streamlined in terms of the comments received.
Roles and responsibilities	• Request that the governing body be defined in the standard • Clarification of the oversight function of the board. • Clarity regarding delegation of the governing body's responsibilities • Clarity on who is referred as third-party service providers • Clarity around the role and responsibility of the cyber and information security function	• The definition of governing body in the Financial Sector Regulation, Act – and is comprised of both executive (C-Suite) and non-executive directors. • The delegation of responsibility is an internal matter best handled by the institution. The Authorities will, however, hold governing body ultimately responsible for compliance with this Joint Standard. • A third party is anyone that is not the financial institution or part of the group to which the financial institution belongs. • Paragraph about the roles and responsibilities of the cyber and information security function has been amended to make this clearer:
Governance	• Clarification on the role of the information security function in relation to non-digital information, as well as all cyber and information security issues within a financial institution. • Clarification on whether the function can be split as well as who has oversight over the function. Clarification of whether the oversight function must be independent.	• The definition of information asset has been augmented to state that it excludes paper-based information. The cybersecurity definition in the Joint Standard does cover information in so far as it refers to data that is based on a digital medium. • It must be demonstrated to the Authorities that a function (s) has/have been established or exists that deals with cyber and information security. The paragraph has been amended to make this clearer. In addition, the Joint Standard has been amended to empower the Authorities to prescribe separate functions if the nature, scale, complexity and risk profile warrants such a separation. • In addition, the Authorities have inserted a paragraph 6.2 to enable the Authorities to require a financial institution based on its nature, scale, complexity and risk profile to have an independent oversight function'.
Cybersecurity strategy and framework	• Clarification on whether the cybersecurity strategy and framework must be separate documents or whether it can be	• Where an institution has an enterprise risk management framework, it may incorporate the requirements into the framework provided that its incorporation is demonstrable to the Authorities.

Table 4 – Summary of comments received from the consultation conducted in 2023		
Paragraph of the Joint Standard	**Summary of comment s**	**Response from the Authorities**
	combined with existing documentation. • In terms of references to industry best practice/standards, will the Authorities prescribe the relevant best practices. • The timing, purpose and necessity of an annual independent review of the security framework was also raised.	• The Authorities will not recommend industry best practice or standards. However, the Authorities will assess the standards applied based on the nature, scale, complexity and risk profile. Financial institutions must discuss the role of industry bodies in terms of best practice. • Due to the nature of the risk related to cybersecurity and resilience, it is imperative that the review is conducted at least annually by an independent function such as risk, compliance or internal audit. Financial institutions can also appoint an external auditor. The purpose of the review is to ensure adequacy and effectiveness of the framework.
Cybersecurity and cyber resilience fundamentals	• General drafting suggestions were made to eliminate confusion. • Due to the complexities of certain applications and rapid development and releases, it may not be feasible to implement such an approach in every phase of software development. • Concerns regarding sharing information with other industry players in order to create awareness, note trends etc on cyber security. • Concerns on how an institution will “ensure” on environments that they have no control over and will not have constant monitoring on especially in the case of third-party service providers. • Encryption is resource intensive and may not even work on some legacy systems and databases	• Security measures must be developed in every phase to ensure the security of the holistic application. This also ensures that security and loopholes (vulnerabilities) are considered at every leg of development. Due to the various financial institutions to which the Joint Standards applies, the security-by-design approach is based on the nature, scale, complexity and risk profile of the financial institutions. The Authorities do not prescribe to one specific model. Supervisory discretion will be applied on assessment of the approach. • Institution specific or customer specific information will not be shared, it is more the modus operandi, trends, lessons, indicators of compromise, challenges etc. Financial institutions should engage in such arrangements to strengthen their cyber defence and resilience such as participation in industry CSIRT/ CERT, involved in committees such as CRS forums and industry association forums that deal with industry risk. • This is a minimum requirement of the Joint Standard as third-parties have access to the information and systems of the financial institution. This can be established when the financial institution does its due diligence on a service provider before entering into a contract.

Table 4 – Summary of comments received from the consultation conducted in 2023

Paragraph of the Joint Standard	Summary of comment s	Response from the Authorities
	without extensive upgrades and re-architecture. • Suggestion to add a requirement to review firewall rules on a periodic basis and adding a requirement to test network perimeter controls and posture at least annually by certified professional • Not all organisations can establish or afford a Securities Operations Centre. A good monitoring and incident response team can be just as effective. • Clarification whether cloud service providers apply to offline/offsite backups. • Recommended that reference to black box, grey box and white box testing be deleted as this will have a significant financial impact on the financial institution.	• The Joint Standard was amended to require that sensitive information stored in systems and endpoint devices is encrypted and protected by access control mechanisms commensurate to the risk exposure. • The Authorities added a requirement to review firewall rules on a periodic basis as well as to test network perimeter controls and posture at least annually. • The paragraph has been amended to enable the establishment of security monitoring capabilities, such as a security operations centre (or similar), or acquire managed security services, in order to facilitate continuous monitoring and analysis of cyber events as well as prompt detection and response to cyber incidents. • The offsite location includes cloud storage services. The Joint Standard has been amended to include cloud storage. • The paragraph has been amended to remove the requirement for black/white/grey box testing to be done but to include an enabling provision to the effect that the Authorities may, based on the nature, scale, complexity and risk profile of the financial institution specify that a black box, white box, grey box testing or a combination thereof.
Cybersecurity hygiene practices	• Comments on the cost of segregation of duties for smaller FSPs, the limitation of the requirements to only critical systems as well as the possibility of passwordless authentication. In general, there were comments on the prescriptive nature of the requirements. • Clarification and comments on the application of the requirements to third party service providers and the cost	• The Joint Standard contains minimum requirements for cyber security and cyber resilience. The Joint Standard was amended to cater for tokens and biometric enabled access. The prescriptive of the requirements are necessary due to the significant impact of cyber-incidents and cyber-attacks. • Third party providers must implement the same or equivalent security controls as the financial institution. It is the responsibility of the financial institution to ensure that the third-party service provider has the necessary securities in place. • General drafting suggestions were accepted where appropriate and relevant.

Table 4 – Summary of comments received from the consultation conducted in 2023

Paragraph of the Joint Standard	Summary of comment s	Response from the Authorities
	implications on the 3rd Party providers which may not be recoverable. • General drafting suggestions were also made.	
Reporting	• The request is for the Authorities to provide guidance on the parameters of what is deemed 'material' in the context of the proposed Joint Standard. • Institutions are concerned that there is a duplication of the requirements as set out in Directive 2 of 2019 and recommended that it be removed. • Concerns that 24hours is not practical for reporting incidents. We should rather consider "as soon as reasonably possible". As well as the threshold to report, if a report must only be made after classifying the event as material, what would the consequences be if a financial institution did not classify the event in question as material and therefore did not report to the Authorities. Clarity if the Authorities will later question the financial institution's characterisation of the event as non-material and what the consequence of an incorrect classification be? • The was a request that the reporting template should to be	• The institution is responsible for classifying material system failure and malfunctions. • Directive 2 will be repealed when the Joint Standard is finalised. • 24 hours is only after classifying the event as material. The reporting template will provide more detail on the information required. The paragraph has been amended in respect to the 24 hours. • The form of reporting as well as the timing will be communicated in the reporting template which will be published for comment during the formal consultation process. • As these are being dealt with by different regulators with different mandates, dual reporting is required where necessary.

Table 4 – Summary of comments received from the consultation conducted in 2023

Paragraph of the Joint Standard	Summary of comment s	Response from the Authorities
	defined and attached as an addendum to the proposed Joint Standard for comment. • Request for reporting to be provided to the responsible authority rather than to both Authorities.	
General comments	• Clarity about the process FI's to follow to apply for exemption from any of the set standards. • Concern that there is no mention of POPIA in the Standards (only the FSR Act). • Clarity if IR's authority will take precedence over the FSCA / PA in the event of an investigation / incident or breach? • Clarity on the penalties for FI's in the event of breach / non-compliance to any of the standards. Concerns about conflating technology risk, information risk, cyber risk and information security in one Standard	• The process for exemptions is catered for in terms of section 281 of the Financial Sector Regulation Act. • The regulators have different mandates. The financial institution must comply with the requirements imposed by the different regulators. • These are dealt with in terms of the FSR Act and the regulatory action policies of 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.

Table 5 – Details of commentators that commented in the consultation in 2021

Name of organisation	Contact Person and Contact Details
Clientèle Limited (including Clientèle Life Assurance Company Limited and Clientèle General Insurance Limited)	Malenthren Govender
Habib Overseas Bank Limited	Rehan Zaidi / Neo Motlagomang
Standard Bank Group	Robin Barnwell
Masthead	Anri Dippenaar
Bank Zero Mutual Bank	Jayesh G Prag
Bank of China	Rookeya Salajee
Willis Towers Watson	Dr Erich Potgieter (Associate)
BASA	Benjamin April
Deutsche Bank AG	Johan Gibhard
Assent	Freddie Eilers
Alan Gray	Werner Lunow
ASISA Association for Savings and Investment - South Africa Consolidated submission on behalf of ASISA Members	Johann van Tonder
Silica Administration Services (Pty) ltd	Eugene Venter
FirstRand Group	Kovelin Naidoo
Nedbank Limited	Lianca du Toit
Financial Intermediaries Association of Southern Africa (FIA)	Samantha Williams
BrightRock	Lyton Simbanegavi
Bidvest Bank	Jaco De Beer
Equity Express Securities Exchange (Pty) Ltd	Nikki Clackworthy
Johannesburg Stock Exchange	Anne Clayton
The Federated Employers Mutual Assurance Company (RF) (Pty) Ltd	Gys Mc Intosh
Purple Group Limited (“Purple Group”)	Sascha Graham
A2X Markets	Luthfia Akbar/ Gary Clarke
SA Home Loans	Mark Dand
MTN SA	Isack Ngobeni
OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	Maretha Hurter
China Construction Bank Corporation Johannesburg Branch	Shannon Delpeche
Investec	Carmel Lerner
Aurora Insurance Company	Angie Botha
ENSAfrica	Rakhee Dullabh, Jessica Blumenthal
Just Retirement Life (South Africa)	Thiren Pillay

The Cape Town Stock Exchange	Hannes van der Merwe
Integrity Retirement Fund Administrators (PTY) Ltd	Fritz Wasserfall
The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	Ntsoaki Ngwenya
Hollard	Ntokozo Magasela
AIG	Fiona Oakley-Smith
Institute of Retirement Funds Africa	Wayne Hiller van Rensburg
Rand Mutual Assurance	Juanita Moolman & Ben Lourens
Two Mountains	Lindani Ngema
CITIBANK NA SOUTH AFRICA	Edward Kiptoo

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
1.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	1	No comment	Noted.
2.	Hollard	1.	i. We propose that a transitional period, to enable organisations to perform a detailed gap analysis of existing controls against the proposed Joint Standard, be considered. ii. We propose that thereafter, based on the feedback from the various organisations in terms of the detailed gap analysis, that a further transitional period affording organisations to establish baseline compliance with the proposed Joint Standard, be considered. We propose a staggered approach to implementation, with milestones, be considered. We fully support the need for this standard as well as for all financial institutions to build strong cyber resilience given the increasing prevalence of cyber-criminal behaviour. We do believe though the more	Noted. It is the view of the Authorities that an 12-month transitional period is adequate for preparation to ensure full compliance with this Joint Standard. The Joint Standard will be published and from the publication date a 12-month period will be given to financial institutions to implement the requirements of the Joint Standard. Noted, however due to the risk implications, the Authorities are of the view that the 12-month period will provide sufficient time for readiness.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			important actions that need to be prioritized are the actual building of systems and capability to track, test and defend incursions. The formal policies and strategies can perhaps come later and as with the PPR and Binder Regulations where there was a staggered implementation period, we would support the same here. Policies and strategies take time, the defending of critical data is a joint effort between all stakeholders to be done as quickly as possible.	
3.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	1.	• We noticed that there is no provision for a transitional period Based on the information at our disposal we will require time to adhere to all the requirements introduced, which will require additional control and possibly staffing resources, we request the consideration of 12 months transitional period to be introduced.	Noted. It is the view of the Authorities that an 12-month transitional period is adequate for preparation to ensure full compliance with this Joint Standard. The Joint Standard will be published and from the publication date a 12-month period will be given to financial institutions.
4.	Aurora Insurance Company	1.1	Is there any indication as to the actual commencement date and is there any expectation of	See response to comments 2 and 3 above. The revision depends on comments raised.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			another revision of the Joint Standard before commencement?	
5.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	2	No comment	Noted.
6.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	2	No comment	Noted.
7.	Aurora Insurance Company	2.1	Duly Noted.	Noted.
8.	Standard Bank Group	2.1	There is a definition of “the Act” after this statement. Financial Sector Regulation Act should be referenced in this statement to avoid confusion, as the definition comes after.	Noted, the Joint Standard has been amended to capture the full name of the Act.
9.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	3	No comment	Noted.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
10.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	3	We have noticed that the draft standard only refers of 3rd party service providers in paragraph 8.2.3 (a) (iii).	The Joint Standard does not apply directly to third-party service providers, however where a financial institution is utilising the services of third parties, the security controls of the third-party must be equivalent to that of the financial institution.
11.	Aurora Insurance Company	3.1 – 3.5	Duly Noted.	Noted.
12.	Investec	3.2	In reference to Juristic person and branches structured under the bank or controlling company, it is not clear if this only applies to those within the South African jurisdiction.	The Joint Standard applies to the South African registered entity and requires the entity to consider any potential risks relating to cybersecurity and cyber resilience 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. It applies to subsidiaries and branches within and outside the Republic. The paragraph has been amended to make it clear that it applies within and outside the Republic.
13.	BASA	3.2 and 3.3	Recommend that “potential risks” be updated to “material risks.” “A financial institution that is a bank, or a controlling company must ensure that any potential risks relating…”	Noted. However, the Joint Standard covers all risks relevant to the subject manner and it is intended that the financial institution must consider all risks and mitigate according to the nature of the risks. In order to eliminate any confusion, the word ‘potential’ in relation to risks has been deleted.
14.	First rand Group	3.2 and 3.3	“A financial institution that is a bank, or a controlling company must ensure that any **potential risks** relating…” We recommend that “potential risks” should be updated to “material risks”.	See response to comment 13 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
15.	Investec	3.4	Ambiguity as to whether these are the minimum requirements that must be implemented in full, or proportional to risk appetite / size / complexity of the institution. In addition, it is unclear if this standard supersedes internationally recognised security frameworks (e.g., ISO27001, NIST CSF) that an institution currently follows.	The Joint Standard contains the minimum requirements and principles issued to financial institutions by the conduct and prudential regulatory. The best practices were considered in the drafting of the Joint Standard and the requirements should not be contradictory but may in some cases be more onerous than best practice. In addition, to ensure clarity, paragraph 3.4 and 3.5 has been amended by: (i) adding principles to paragraph 3.4 and (ii) merging with paragraphs 3.5 with 3.4 and stating that 'The minimum requirements and principles of this Joint Standard must be implemented to reflect the nature, size, complexity and risk profile of a financial institution. To consider adding that 'appropriate, adequate, effective, timely' will be assessed in terms of the nature, complexity, scale, risk profile of the financial institution.
16.	Johannesburg Stock Exchange	3.4 & 3.5	Paragraphs 3.4. and 3.5 are contradictory provisions. Paragraph 3.4 provides that the requirements set out in the Joint Standard are 'minimum requirements', i.e., a financial institution must, as a minimum, comply with all of the provisions of the Joint Standard. Paragraph 3.5 provides for flexibility in the application of the Joint Standards: the requirements may be 'implemented in accordance with the risk appetite, nature, size and complexity of a financial institution'. However, no provision is made for the method	Refer to response to comment 15 above. The Authorities do not subscribe to one particular international framework/standard and has considered a number of international standards/best practices (including CPMI-IOSCO) in drafting the minimum requirements and principles contained this Joint Standard.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			or approach a financial institution should use to assess which requirements may be implemented with discretion. These two provisions are contradictory as it would be impossible for a financial institution to comply with rule-based prescriptive requirements concurrently with flexible risk-based requirements for the sake of proportionality. With reference to our general comment (3) below, we are of the view that the Joint Standard should simply require that a financial institution should implement a cybersecurity and cyber resilience framework aligned to one of the three internationally accepted standards. In particular, we recommend that market infrastructures should be required to implement a cybersecurity and cyber resilience framework aligned to the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures. This preferred approach would enable financial institutions to leverage off of existing frameworks and infrastructure and implement standards in accordance with the	

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			risk appetite, nature, size and complexity of that financial institution. Supervision by the Authorities of a market infrastructure's compliance with the Joint Standard, would be more efficiently focussed on the market infrastructure's compliance with the PFMIs, rather than monitoring whether each prescriptive requirement in the Joint Standard has been complied with.	
17.	Hollard	3.5	This clause requires further clarification, as it is subjective and open to interpretation.	See response to comments 15 and 16 above.
18.	Willis Towers Watson	3.5	Given that the draft Standard is otherwise highly prescriptive, clear and detailed guidance is needed as to how financial institutions should interpret and apply this paragraph, i.e. the statement that "[t]he requirements … must be implemented in accordance with the risk appetite, nature, size and complexity of a financial institution." At the risk of labouring the point, it is impossible for a smaller, less complex or what we term below a "downstream" financial institution to know how to interpret the numerous	See response to comments 15 and 16 above. Smaller financial institutions must approach the PA when they are concerned with their compliance with the Joint Standard. If the dispute is because of interpretation issues - an interpretation note may can be issued by the Authorities. If the Authorities take a decision that is not accepted by the financial institution in terms of compliance, then the financial institution can take such decision to the Financial Services Tribunal for review.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			paragraphs of the Standard that start with "A financial institution must…", in the light of para. 3.5. Does para. 3.5 in fact give such institutions leeway not to do (some or all of) the many things which the rest of the Standard says they "must" do? And what will happen when a dispute arises between a particular financial institution and the Authorities, as to whether the institution has complied with the Standard or not?	
19.	BASA	3.5	Recommend implementation according to the risk appetite of the organisation leave a level of openness Recommend making this a guideline and not a standard.	Refer to response to comment 15 and 16 above. The Authorities have removed risk appetite and incorporated risk profile as this is a broader concept. It is not the intention of the Authorities to issue guidance on this critical topic as there is a need for enforceable requirements.
20.	Purple Group Limited ("Purple Group")	3.5	Please provide clarity on the meaning of size? For example is this in relation to the number of employees or the amount of assets under management or amount of sensitive information held? A financial institution may be small in terms of number of employees but may hold significant amounts of sensitive information.	Refer to response to comments 15 and 16 above. Size is intentional broad to cater for various elements. In consideration of significant amounts of sensitive information – this may also fall under complexity and risk profile of an organisation.
21.	Johannesburg Stock Exchange	3.5	The Statement of the need for the Joint Standard (Annexure B) references the consideration of	The exemption process is covered in section 281 of the FSR Act.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			an exemption from a specific requirement of the Joint Standard. However, the Joint Standard does not explicitly provide for an exemption, nor indeed the process to apply for an exemption.	
22.	MTN SA	3.5	This section provides that the requirements of the Joint Standard must be implemented in accordance with the risk appetite, nature, size and complexity of the financial institution. It is important to note that in certain instances, like with MTN SA, the Joint Standard will only apply to a specific business area within the company. This is because MTN SA as a whole is not a financial institution but rather has a business area that provides certain financial services. Therefore, the risk appetite, nature, size, and complexity referred to in this section will only be that of the business area concerned and not of MTN SA in its entirety.	Refer to the response to comment 15 and 16 above. This Joint Standard applies to the registered/licensed entity and the Authorities will ensure that the minimum requirements and principles are adhered to by the registered/licensed entity whether managed from a solo or group perspective.
23.	Investec	3.5	Ambiguity as to whether these are the minimum requirements that must be implemented in full, or proportional to risk appetite / size / complexity of the	Refer to the response to comments 15 and 16 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			institution. And how the implementation will be measured against an institution's internal risk appetite. Contradicts these being positioned as "minimum expectations" i.e., mandatory.	
24.	ENSAfrica	3.5	While this provision provides for proportionality in accordance with the principles of the Financial Sector Regulation Act, 2017 (FSRA), small financial institutions may find it difficult to comply with some of the extensive (and expensive) obligations required under the Joint Standard. Specific exemption in some instances may be required. Do the Authorities intend to provide guidance in this regard or will financial institutions be required to seek exemption on a case by case basis? We are thinking particularly of emerging discretionary financial services providers who often struggle to ensure compliance as they are relatively small organisations in size, albeit that the nature of their business may be complex.	If the Authorities identify a need, a guidance notice may in terms of the provisions of the FSR Act be issued. The Joint Standard prescribed minimum requirements and principles on the subject matter and the expectation is that all captured financial institutions must comply. Exemptions are dealt with in terms of the provisions of section 281 of the FSR Act.
25.	MTN SA	3.6	The Joint Standard must also be read in accordance with the specifications as outlined in the Cybercrimes Act 19 of 2020. It is	Noted, however, the Authorities do not want to specify a particular piece of legislation as in future this list may increase, and the Joint Standard will thereafter become limited. In addition, it will be

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			the recommendation of MTN SA that this be highlighted in the proposed Joint Standard.	impractical to specify all the applicable legislation that have common areas of application.
26.	Hollard	4. Definitions and interpretation/ 4.1	We propose including a definition of 'breach', as being distinct from the definition of 'compromise'. Not all compromised security systems result in a data breach.	The Joint Standard does not use the term 'breach' rather the 'term' compromise' as such term is broader than events covered by a 'breach'.
27.	Hollard	4. Definitions and interpretation/ 4.1 'cyber incident' (b)	Unless the violation results in Compromise or Breach, this is a Cyber Event, not a Cyber Incident. Business as usual operations may intercept employees that inadvertently violate a security policy. The processes and controls put in place mitigate the Cyber Event from becoming a Cyber Incident, avoiding a Compromise or Breach.	That the Joint Standards clearly distinguishes between a cyber event and a cyber incident. The Authorities are of the view that once the security policy has been breached it is an internal cyber-incident whether there is compensating controls or not.
28.	Hollard	4. Definitions and interpretation/ 4.1 'indicators of compromise'	Indicators of compromise (IOCs) are not only used to identity that a cyber incident has occurred in the past, or that a cyber incident is occurring. IOCs are extensively used to assist in preventing a cyber incident from occurring. IOCs are added to security software to detect and prevent the related cyber incident.	The Authorities are of the view that the definition of IOC is adequate for the use of the concept within the Joint Standard.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
29.	Hollard	4. Definitions and interpretation/ 4.1 'security controls'	Add "or cyber event" to the end of the definition.	Noted and agreed. 'Cyber-event' has been added to the end of the definition of security control.
30.	Hollard	4. Definitions and interpretation/ 4.1 'security'	Include a definition of information security. The definition of cyber security is already included.	Noted and agreed. A definition for information security has been added to the Joint Standard. Information Security – means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide— 1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. 2) confidentiality, which means preserving authorized restrictions on access and disclosure, including the protection of privacy and proprietary information; and 3) availability, which means ensuring timely and reliable access to and use of information.
31.	Johannesburg Stock Exchange	4. Definitions: 'information asset' 'IT infrastructure'	The definition of 'information asset' is extremely broad, particularly in respect of the definition of 'IT infrastructure'. '**information asset**' means any piece of data, device or other component of the environment that supports information-related activities. In the context of this Joint Standard, information assets include data, hardware and software; **'IT infrastructure'** means a set of hardware, software and	Noted. The Authorities are of the view that since the Joint Standard is related to information technology and information that sits on information technology platforms and no other types of information. The definition of 'IT infrastructure' has been amended to replace information asset with IT system.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			facilities that integrates a financial institution's information assets; An information asset may not in all instances be integrated by an IT infrastructure and a financial institution may not in all instances be in a position of oversight of such information assets and/or IT infrastructure. In addition, clarity is required regarding what constitutes "support" of information-related activities.	
32.	Johannesburg Stock Exchange	4. Definitions: 'sensitive information'	The definition of 'sensitive information' does not make specific reference to 'confidential information' as defined in the Financial Markets Act ('FMA'). We recommend that the scope of this definition should be extended to include a reference to 'confidential information', as defined in the FMA, given that the consequences of a breach/disclosure is prescribed as an offence in the FMA. In the Joint Standard reference to sensitive information is made in clause 9.3.1(c) in the context of multi-factor authentication (MFA). The Joint Standard otherwise references and uses the term 'sensitive data' throughout. For the sake of	. Noted, to ensure consistency – sensitive data has been changed to sensitive information. The definition of sensitive information has also been amended to say: means information or data where loss, misuse, or unauthorised access to or modification of could adversely affect the public interest or a financial institution or the privacy to which individuals are entitled.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			clarity and consistency, we recommend that either of the terms 'sensitive information' or 'sensitive data' is used throughout the Joint Standard.	
33.	Aurora Insurance Company	4.1	Duly Noted.	Noted.
34.	Investec	4.1 "attack surface"	Propose using the NIST definition which is clearer: "The set of points on the boundary of an IT system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment".	Noted. The Authorities are of the view that the current definition is adequate for the context of the Joint Standard. The Prudential Authority has previously used this definition in other regulatory instruments.
35.	Investec	4.1 "black / grey / white box testing"	Suggest removing this definition (and reference to the different testing types in 8.6.3i) as it non-essential and adds complexity. Keep the requirement clear in that penetration is required.	Noted. 8.6.3 - The paragraph has been amended to remove the requirement for black/white/grey box testing to be done but to include an enabling provision to the effect that the Authorities may, based on the nature, scale, complexity and risk profile of the financial institution specify that a black box, white box, grey box testing or a combination thereof be conducted. The scope being IT system and information assets will remain in the requirement.
36.	Investec	4.1 "compromise"	Would add "or data" as the word compromise can apply to both systems and data.	Noted. The definition of compromise has been amended to include information asset which includes data.
37.	Investec	4.1 "cyber event"	Definition is too broad. Propose adding more detail, e.g., "any observable occurrence in an IT system that may be indicative of an actual or attempted	The definition used in the Joint Standard comes from the Cyber Lexicon and does not mean that every observable occurrence results in a cyber incident.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			cyberattack". "Observable occurrence" could for example be running out of disk space, which should not qualify as a cyber event.	
38.	Investec	4.1 "sensitive information"	Typo – should be "adversely affect the public interest **of** a financial institution"	Noted and agree. The typo has been rectified.
39.	Institute of Retirement Funds Africa	4.1 definition of 'financial institution'	Due to the manner in which the governance, management and operations of a pension fund are structured there it is recommended that an additional organisation is included in the definition: "An administrator as licensed under the Pension Funds Act, 1956 (Act 24 of 1956)"	Although, we agree with your proposal in principle, the Authorities are concerned that extending the scope of the Joint Standard would constitute quite a material change that was not consulted on previously. Accordingly, the Authorities will not address the proposal at this stage, considering where we are from a process perspective in making the Standard. Authorities will consider whether alternative measures are available to address this issue, which could include a possible amendment.
40.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	Definitions and interpretation (4)	No comment	Noted.
41.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	Definitions and interpretation (4)	• The standards make reference to 3rd party service provider. We request that it be included in the definitions and interpretation section.	A third party is not the financial institution. The Authorities are of the view that this term does not need to be defined. Any issues around the identification of the third party can be referred to the PA or FSCA for guidance. The Joint Standard does not use the term 'breach' rather the 'term' compromise' as such term is broader than events covered by a 'breach'.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			• Consider using the definition "Breach" instead "Compromise" The definition "Cyber Incident" needs to include information security as well now that the definition of security in terms of this draft standard states both cyber and information security. Furthermore, this draft standard needs to consider the inclusion of data breach from a privacy law perspective.	The cyber incident definition also refers to information. The Authorities are of the view that there is no need to incorporate information security specifically in the definition. The POPIA will deal with privacy law matters.
42.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	Roles and responsibilities (5)	No comment	Noted.
43.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	Roles and responsibilities (5)	No comments	Noted.
44.	MTN SA	5	The section refers to a "governing body", however the definitions section under section 4 does not provide a definition of what would constitute a "governing body". For the	Noted. The definition of a governing body is provided in the Financial Sector Regulation Act, 2017.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			avoidance of uncertainty, it is the recommendation of MTN SA that the definition of "governing body" be clearly defined.	
45.	Rand Mutual Assurance	5 – Roles and Responsibility	The role of the Chief Information Officer is not mentioned – is there a reason for omitting the CIO (or IO) from ensuring cyber resilience is implemented and maintained in the financial institution?	Not all financial institutions in scope of the Joint Standard will have a Chief Information Officer.
46.	Bidvest Bank	5.	It is recommended that section 5 of the Joint Standard state that all of the governing body's responsibilities may be delegated.	Delegation is an internal matter best handled by the institution. The Authorities will, however, hold governing body ultimately responsible for compliance with this Joint Standard.
47.	Bidvest Bank	5.1	"Governing Body" is not set out in the Definitions and Interpretation section of the Joint Standard.	See response to comment 44 above.
48.	Investec	5.1	Is there a level defined where the required governing body should sit at, i.e., management level, c-suite, etc. or does this refer to overall board accountability within financial institutions	See definition of governing body in the Financial Sector Regulation, Act – and note that a governing body is comprised of both executive (C-Suite) and non-executive directors
49.	Aurora Insurance Company	5.1 – 5.2	Duly Noted.	Noted.
50.	Financial Intermediaries Association of Southern Africa (FIA)	5.1 - Roles and Responsibilities	Governing Body – this term needs to be better defined as what constitutes a governing body in a large organisation may	See response to comment 44 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			be very different for a smaller organisation.	
51.	BASA	5.1.2	Only this statement in section 5 indicates that a governing body may delegate this responsibility. Recommend that the governing body should be permitted to delegate all the other responsibilities listed in section 5. Recommend including in 5.1 that the governing body may delegate where necessary any of the responsibilities. This does not relieve the governing body of accountability, but it does allow them to focus on the full set of risks facing the financial institution and for senior management to fulfil their rightful role in the running of the firm.	Noted, however delegation below the governing body level is an internal matter.
52.	BASA	5.2.2	Recommend the inclusion of the definition of "Systemic Cyber Resilience" in section 4, Definitions and interpretation.	Noted, the Joint Standard has been amended to remove the word 'systemic' and add the words 'financial sector' and to replace the word 'ensure' with 'enable resilience'.
53.	Johannesburg Stock Exchange	5.2.3	With reference to our response to Question 4 below in respect of transitional arrangements, we suggest that the requirement to ensure that roles and responsibilities for security are clearly defined in the contract or Service Level Agreement with third-party service providers, provides for the prioritisation of	Financial institutions will be provided with 12-months within which to implement the Joint Standard and they are free to prioritise which contracts must be amended first.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			material contracts with third-party service providers. We note also that the cost of compliance of amending existing contracts with third-party service providers will be borne by the financial institution and the compliance costs incurred by the third-party service provider may also be passed to the financial institution.	
54.	BASA	5.2.3	Clarify what minimum oversight and assurance requirements are sufficient. Recommend aligning the standard with the SARB outsourcing and 3rd party risk management directives. Recommend defining 3rd parties and align the definition with existing SARB directives. Roles and responsibilities are defined in contracts and Service Level Agreements with 3rd party service providers. Third-party obligations do include cyber and information security requirements. It is unclear whether this refers to security service providers, IT or infrastructure service providers, or others. Refer to 'ensure that roles and responsibilities for security are clearly defined in the contract or Service Level Agreement with third-party	Security means both cyber and information security and not physical security in general. Please see definition of 'security'. There is no definition of third-party service providers in the Banks Act directive. A separate standard will be issued for outsourcing.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			service providers' - the current wording can be interpreted that the governing body should review individual contracts with 3rd party service providers. Recommend that the wording state that the governing body should ensure that a process is in place to clearly define security roles and responsibilities with 3rd parties. Contract for an EDC may differ from the contract for AWS	
55.	First rand Group	5.2.3	Roles and responsibilities are defined in contract or SLAs with 3rd party service providers – it is unclear whether this refers to security service providers, IT or infrastructure service providers or other. 3rd parties should be defined.	Security is defined in the Joint Standard and means cybersecurity and information security.
56.	Financial Intermediaries Association of Southern Africa (FIA)	5.2.3 – Third Party Service Providers	Third Party service providers needs to be better defined, for example, does this also apply to Microsoft, Sage / Pastel, etc.	The requirement applies to all service providers that will have an impact on a financial institution's cybersecurity risk and cyber resilience capabilities. Further, a third party is anyone that is not the financial institution or part of the group to which the financial institution belongs. The governing body may delegate this function to senior management to ensure that the roles and responsibilities are clearly defined.
57.	**6. Governance**			
58.	OUTsurance Holdings Limited, OUTsurance	6	No comment	Noted.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
	Insurance Company Limited and OUTsurance Life Insurance Company Limited			
59.	Hollard	6.1	Duly Noted.	Noted.
60.	Standard Bank Group	6.1	Proposed addition to Governance: Ensure that a fit and proper person is appointed as the accountable party responsible to lead the financial institution's Security Programme. This person should be empowered and supported to drive the financial institution's Security Programme.	Noted, however, the financial institution depending on the nature, size, complexity and risk profile, may appoint a person to lead the financial institution's Security Programme. Due to the fact that this Joint Standard applies to smaller institutions as well, it is not preferable to hard code such a requirement. Standard Bank is welcome to appoint such a person. Also please refer to the paragraph 7.3(i) of the IT Risk and Governance Joint Standard which specifically requires all staff dealing with the IT System – to be fit and proper.
61.	Institute of Retirement Funds Africa	(6.1.2 and 6.1.3)	Proper guidelines of how cyber risk management will be incorporated into the governance and risk management structures should be communicated.	Although the provision is couched in peremptory terms and is explicit in its import, the Authorities envision that a financial institution will apply its discretion relative to its governance arrangements. At this stage the Authorities do not envision that guidance is required. Also see response to comment 76 below.
62.	BASA	6.1.3	Reference is made here to an information security function. Recommend defining information security or an information security function definition in section 4 of this document. Recommend that it is important to exclude any non-digital information protection. Recommend including the	Noted. A definition for information security has been inserted. The definition of information asset has been augmented to state that it excludes paper-based information. The cybersecurity definition in the Joint Standard does cover information in so far as it refers to data that is based on a digital medium. Paragraph 6.1.4 covers the information security function as a second line of defence as it calls for independence. The Joint Standard prescribes minimum requirements for cybersecurity and cyber resilience,

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			definition of cyber security within the context of Information security function and responsibilities. Furthermore, this statement stipulates that the information security function is responsible for all cyber and information security issues. Prudential regulations are structured around a Three Lines of Defence model (first line) frontline, (2nd line) risk and compliance, and (3rd line) audit. It must be noted that the first line is always responsible and accountable for any risk. Recommend that consideration must be given for information security functions which are 2nd line functions. Furthermore, organisations may have established cyber risk functions. Prescribing the roles of functions may force changes to an organisations operating model. Regulations in different countries may attempt to define roles differently creating additional organisational complexity for financial institutions which is a barrier to good security and resilience. It is good practice to avoid prescription regarding the organisational structure of the	these minimum requirements must be complied with by the financial institution in terms of policies, procedures and processes. It must be demonstrated to the Authorities that a function has been established or exists that deals with cyber and information security. Paragraph 6.1.3 has been amended to make this clearer: ensure that a function(s) responsible for cyber and information security operations is established with adequate resources and appropriate authority. Amended 6.1.4 to: ensure that the oversight of the function(s) referred to in paragraph 6.1.3 above has access to the governing body and is structured in a manner that ensures adequate segregation of duties and avoid any potential conflicts of interest. See response to comment 69 below.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			financial institution in favour of a focus on the results regulators seek to achieve. Clarify the roles and responsibilities for cyber security and information security (is cyber security a subset of information security or vice versa). Recommend enhancing the wording to "ownership and responsibility for cyber and information issues is clearly defined and understood within the organisation." In this way, organisations may allocate based on the operating model.	
63.	BASA	6.1.3	**Clarify** what does "This function must be responsible for all cyber and information security issues within the financial institution**."** The current wording is too broad. **Clarify** is the information security function responsible for the resolution of all cyber and information security issues or overseeing the management of the resolution thereof.	Noted, the paragraphs 6.1.3 and 6.1.4 have been amended to make these roles clearer. See responses to comments 61 above and 69 below.
64.	BASA	6.1.3	This says "an" information security function which indicates a single function. This could have a major impact on how the organisation is structured, as often the technical skills lie elsewhere and as such the responsibility for a control could	Noted, the paragraphs have been amended accordingly.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			exist in the Networks or Cloud teams. **Recommend** that it would be more inappropriate to have two distinct functions working closely together, one responsible for Information Technology and the other Cyber security issues. **Recommend** that the context of enterprise risk management practices and Cyber security frameworks be taken into consideration.	
65.	First rand Group	6.1.3	Reference is made here to an information security function. The document does not define information security or an information security function. Suggest including these definitions in section 4 of this document. Furthermore, this statement stipulates that the information security function is responsible for all cyber and information security issues. It must be noted that first line is always responsible and accountable for any risk, so consideration must be given here for information security functions which are 2nd line functions. Furthermore, organisations may have established cyber risk functions. By prescribing the roles of	Refer to response to comment 61 above. Although the Joint Standard does provide specific requirements, the Joint Standard sets out general and overarching principles. Further, paragraph 4.3 of the Joint Standard provides that the requirements of this Joint Standard must be implemented in accordance with the risk appetite, nature, size and complexity of a financial institution.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			functions, it forces organisation to organise itself based on this directive. Suggest re-wording to something like “ownership and responsibility for cyber and information issues is clearly defined and understood within the organisation”. In this way, organisations may allocate based on operating model. It is important to exclude any non-digital information protection from this paper. Include definition of cyber security within the context of Information security function and responsibilities. Roles and responsibilities for cyber security and information security must be made clear (is cyber security a subset of information security or vice versa).	
66.	First rand Group	6.1.3	What does “**This function must be responsible for all cyber and information security issues within the financial institution”**? The current wording is too broad – is the information security function responsible for the resolution of all cyber and information security issues or overseeing the management of the	See response to comment 61 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			resolution thereof. Clarity on the expectation is important.	
67.	First rand Group	6.1.3	This says "an" information security function which clearly indicates a single function. Would it therefore be inappropriate to have two different functions responsible for Information Technology and another for Cyber security issues? With a close working environment. Also consider context of enterprise risk management practices and Cyber security frameworks.	See response to comment 61 above. Please note there is nothing in this provision precluding a financial institution from having two different functions for IT and Cyber security. At issue is that there must be appropriate oversight and access to the governing authority.
68.	First rand Group	6.1.4	"ensure that the governance and oversight of the information security function is independent from operations to ensure adequate segregation of duties and avoid any potential conflicts of interest." Does this mean that the information security function itself must be independent from operations or does it mean that the function that is responsible for governance and oversight of the information security function (e.g., the 2nd line cyber risk management function) must be independent from operations? Clarity in this regard is important to ensure that the information security function is appropriately	See response to comment 61 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			structured in line with regulatory expectations.	
69.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	6.1.4	• Paragraph 6.1.4 makes reference to an "Information Security Function" that must be separate from the operations. Does this imply a different function such as Compliance, Risk management, Actuarial, Audit which is the second and third line? We request clarity in this regard	This paragraph has been amended to cater for smaller financial institutions and an enabling provision has been included to require separate functions in larger financial institutions
70.	ASISA	6.1.4	There could be confusion to which operations this refers too. If it is security operations, many Financial Institutions might not have sufficient resources to comply with this. Some will have an information security function that performs Governance and Oversight functions, but also provides Security Operations Centre functions (Detection and Response). Sometimes the information security function and the IT Risk management functions are one, or report into one individual – instead of a fully independent function. Paragraph 6.1.4 should be amended for the sake of clarity:	Noted, the paragraph has been amended accordingly. In addition, the Authorities have inserted a paragraph 6.2 to enable the Authorities to require a financial institution based on its nature, scale, complexity and risk profile to have an independent oversight function'.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			-------- ” ensure that the governance and oversight of the information security function is ~~independent from operations to~~ **structure in such a way that it** ensure**s** adequate segregation of duties and avoid any potential conflicts of interest.**”**	
71.	Purple Group Limited (“Purple Group”)	6.1.4	In our view, the independence requirement is not suitable for smaller financial institutions as it requires additional senior resources and segregation of functions which a smaller financial institution might not be able to afford. We respectfully submit that the Authority considers limiting this requirement to financial institutions where it is appropriate for an independent function to exist such as a bank or large insurer.	Noted, the paragraph has been amended. See response to comment 69 above.
72.	Investec	6.1.4	Propose to remove the reference to “governance”. Agree that oversight (i.e., level 2 and 3) must be independent from security operations; but disagree that the governance of cyber must be independent. It is possible, and sometimes preferable, for the governance of cyber to be managed by and within the security function itself.	Governance in this paragraph refers to the way the implementation is executed, resourced etc. We are not referring to operational governance but governance in reference to oversight. However, the Authorities have deleted the word governance in order to eliminate any potential confusion.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
73.	China Construction Bank Corporation Johannesburg Branch	6.1.4 Governance	States governance and oversight of the information security function is independent from operations – would this be interpreted as a) the person who fulfils the responsibilities of ISO must be independent from operations (e.g., IT department) OR b) the persons who provide oversight (e.g. executive or committee) must be independent from the person(s) who fulfil the responsibilities of ISO?	Noted, the paragraph has been amended. See response to comments 69 and 71 above. Independence on the different levels of oversight is necessary in the governance of a financial institution. Both scenarios are therefore correct.
74.	Masthead	6.1.4 – Governance	s6.1.4 We note the requirement that financial institutions must ensure that governance and oversight of the information security function should be independent from operations, and we understand the rationale in relation to potential conflicts of interest. However, while this may be practical in large organisations where there is capacity and/or resources to segregate duties, it provides a challenge in smaller financial institutions/FSPs that are subject to this Joint Standard. We would therefore suggest that the Standard provides for proportionality (as provided for	This paragraph has been amended to cater for smaller financial institutions and an enabling provision has been included to require separate functions in larger financial institutions

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			in s3.5) and discretion in applying the Standard rather than being prescriptive. In order to achieve this, s6.1 could be reworded as follows: 6.1 A financial institution must, where it makes sense in the context of proportionality, … or 6.1 A financial institution must, in accordance with its risk appetite, nature, size and complexity…	
75.	Institute of Retirement Funds Africa	6.1.2 and 6.1.3	Proper guidelines of how cyber risk management will be incorporated into the governance and risk management structures should be communicated.	Noted, the Authorities will assess the need for guidance once the Joint Standard is implemented by the various financial institutions.
76.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	7	No comment	Noted.
77.	Hollard	7. Cybersecurity strategy and framework	To avoid duplication and overlap we suggest that there should be integrated Enterprise Risk Management, Data Management (taking PoPIA into account) and Security Management Governance Framework, and that the	This Joint Standard applies to various financial institutions and not only insurers and contains minimum requirements for financial institutions with regard to cybersecurity and cyber resilience. Where a financial institution has an enterprise risk management framework, it may incorporate the requirements into the framework provided that its incorporation is demonstrable to the Authorities.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			Cybersecurity strategy and framework not necessarily constitute a separate artefact. One needs to bear in mind there is already a Data Policy that needed to be put in place to comply with the Policyholder Protection Rules which also deals with Data Security. The PPR is shortly going to be extended to commercial so there is expected to be considerable overlap with these two policies. We submit the Data policy already in place should be enhanced to include cyber. It needs to be made clear whose overall responsibility it is to implement the mechanisms mentioned in this standard. There are often many links in the supply chain of insurance policies and data which include Financial Service Providers or brokers, third party claims suppliers such as towing operators, panel beaters and salvage dealers and then legal providers such as attorneys and recovery agents. Finally, the reinsurers hold and need to protect a large amount of Insurer data. It would not be optimal for all parties to carry the same responsibilities however	

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			exposures exist in all areas. Must Insurers who ultimately own the data take responsibility for the implementation of what is required in this joint standard and may they force suppliers to co-operate and how are costs to be determined when many parties benefit. To make Insurers responsible for the behaviour of all links in the value chain may not be fair but it needs to be effective over the entire value chain. Clarity in this regard would be appreciated.	
78.	Aurora Insurance Company	7.1 – 7.2	Duly Noted.	Noted.
79.	Just Retirement Life (South Africa)	7.1.1 and 7.1.3	Is the expectation to have two separate documents for the cybersecurity and strategy? As a smaller entity with limited resources, we could have a combined Cybersecurity Strategy and Framework that gets updated and reviewed annually in addition to our existing Information Security and Data Governance policy's which will incorporate all the requirements set out in the standard	Refer to response to comment 76 above.
80.	The South African Insurance Association (SAIA), a	7.1.5	• Paragraph 7.1.5 makes reference to "industry	The Authorities will not prescribe the industry standard. However, through supervision, the Authorities will assess based on the nature, scale,

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
	representative body of the non-life insurance industry		standards and best practices" Clarity is required in respect of where the benchmark will be, i.e., is non-life measured against non-life or is it measured against life insurance and Banks. Furthermore, there are different standards used by different entities which are set by various entities for instance, International Organisation for Standards (ISO) or Critical Security Controls (CSC). Guidance is required from Authorities to provide accredited acceptable standards entities can choose from.	complexity and risk profile whether the industry best practice that is implemented by the financial institution is adequate.
81.	Rand Mutual Assurance	7.1.5 – Policies informed by Industry Standards	Will industry specific standards be set / approved by the Regulator? What role will Industry Bodies play in setting the standards, to ensure consistent standards whereby FI's should measure their own internal policies against?	No, the Authorities will not approve or recommend industry standards. However, the Authorities will assess the standards applied based on the nature, scale, complexity and risk profile. Financial institutions must discuss the role of industry bodies in this regard.
82.	Bidvest Bank	7.1.6	Guidance to be provided on how to quantify business risk tolerance relative to cybersecurity.	This depends on the nature, scale, complexity and risk profile of the financial institution and cannot be prescribed in the Joint Standard. There are various best practices on how this can be quantified.
83.	Investec	7.1.6	Unclear on what is required in the statement "annually define and quantify business risk tolerance relative to	Noted. The paragraph has been amended to read: "Define and reassess regularly business risk tolerance relative to cybersecurity and ensure that

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			cybersecurity" and if a separate standalone statement is expected, in addition to cyber related risk tolerances defined through operational risk management.	it's consistent with the business strategy and risk appetite; and .
84.	Investec	7.1.7	Propose changing the requirement to "information that **informs** reporting", as KRIs / KPIs should serve as input into reporting.	Noted, 'enables' has been changed to 'informs'.
85.	Bidvest Bank	7.2.2	It is recommended that the requirement be amended to state that the Cybersecurity Framework must be reviewed at least annually by the Framework Owner/s, however an adequacy and effectiveness review should only be carried out through independent compliance programmes and audits when the need arises or on an ad-hoc basis when there is a material change to the Framework.	Disagree. Due to the nature of the risk related to cybersecurity and resilience, it is imperative that the review is conducted by an independent function such as risk, compliance or internal audit. Financial institutions can also appoint an external audit. The paragraph has been amended to read: be reviewed regularly, but at least annually, for adequacy and effectiveness through an independent review. A definition of independent review has been added.
86.	ASISA	7.2.2	It is presumed that the required independent review may be performed by an internal control function. The cost and operational impact of an external review, independent of the financial institution, would be unreasonable. Paragraph 7.2,2 should be amended for the sake of clarity:	Noted. See response to comment 84 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			-------- "Be reviewed regularly, but at least annually**, <u>by an internal control function</u>** for adequacy and effectiveness through independent compliance programmes ~~and audits carried out by qualified individuals~~; and"	
87.	Investec	7.2.2	Consider expanding the timeframe. It may be onerous, time consuming, and costly to have the cybersecurity framework independently reviewed / audited every year.	Noted. See response to comment 84 above.
88.	Institute of Retirement Funds Africa	8 (8.2.7) Cybersecurity awareness and training	On the governance side, training will be required on cybersecurity awareness. Similar to the assessments that normally must be completed on the training sites.	Noted and agree.
89.	Hollard	Cybersecurity and cyber-resilience fundamentals/ 8.1.2 (a)	Spelling error: "providerss"	Noted and amended.
90.	Hollard	8. Cybersecurity and cyber-resilience fundamentals/ 8.2.1	Add "or cyber incident" to the end of the paragraph.	Noted, added cyber incident.
91.	Hollard	8. Cybersecurity and cyber-resilience fundamentals/ 8.6.1 (a)	Spelling error: "teffectiveness"	Noted. See revised Joint standard.
92.	Aurora Insurance Company	8.1 – 8.7	Duly Noted.	Noted.
93.	BASA	8.1.1	The way the statement is currently written could be read to imply that the prioritisation will	Noted. Paragraph 8.1.1 has been removed as it has been incorporated in 8.1.2 (b) and (c)

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			be listed from first to last. **Recommend** that this is reworded to read "…organisations should categorise operations and supporting information assets based on criticality and protect these against compromise." Refer to 8.1.2 (b) in this document, which also covers this as well.	
94.	First rand Group	8.1.1	The way the statement is currently written, could be read to imply that the prioritisation will be listed from first to last. Would suggest that this is reworded to read "…organisations should categorise operations and supporting information assets based on criticality and protect these against compromise." Refer to 8.1.2 (b) in this document, which also covers this as well.	Noted. See response to comment 92 above.
95.	Investec	8.1.1	Propose removing this, as it is covered in 8.1.2 (notably 8.1.2c)	Noted. See response to comment 92 above.
96.	First rand Group	8.1.2 (a)	Spelling error - remove the last "s" in "providers"	Noted and amended.
97.	First rand Group	8.1.2 (c)	"carry out risk assessments on its critical operations and supporting information assets to be protected against compromise as well as external	The steps denoted are necessary for the different types of financial institutions to which the Joint Standard applies.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			dependencies, **in order to determine the priority;"** Clarify 'priority" for what purpose? We assume that it would be for risk mitigation purposes as that would be the intention behind a risk assessment. This is a redundant section given that 8.1.2 b stipulated classification of assets which implies risk assessment. Suggest this section is removed.	
98.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	8.1.2(a) & 8.1.3 & 8.2.3(iii) & 8.2.4(a)(i) & 8.2.5(a)(iv) & 8.4.1(d) & 8.5.2(iii) & 8.6.1(b) & 8.6.1(a)(iv) & 8.6.1 (c) & 8.7.1	• Paragraph 8.1.2(a) has a typo; the last word must be providers instead of providerss • Paragraph 8.1.3 refers to inventory; the industry recommends that "Inventory" be defined and made specific toward cyber in order to create uniformity • Paragraph 8.2.3(iii) refer to comment 3 above. • Paragraph 8.2.4 (a)(i) Due to the complexities of certain applications and rapid development and releases, it may not be feasible to implement such an approach in every phase of software	• Noted, the typo has been deleted. • Inventory is unpacked in 8.1.2(d) above. • For the purposes of the Joint Standard, the Authorities are of the view that third parties should not be defined. This applies to anyone that manages your system that is not within the financial institution and not applying the requirements of this Joint Standard. • The Authorities disagree with this proposal and security measures must be developed in every phase to ensure the security of the holistic application. This also ensures that security and loopholes (vulnerabilities) are considered at every leg of development. Due to the various financial institutions to which the Joint Standards applies, the security-by-design approach is based on the nature, scale, complexity and risk profile of the financial institutions. The Authorities do not prescribe to one specific model. Supervisory

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			development. It is therefore requested that "must" is replaced with "should" in consideration of challenges anticipated in meeting this absolute compliance requirement. Furthermore, could the Authorities provide guidance on what standard will the security-by-design approach be judged/ benchmarked? • Paragraph 8.2.5 (a)(iv) This requirement may not be relevant and or an entirely appropriate protection mechanism, considering the wide adoption of the Zero Trust model across the cybersecurity industry; (Zero Trust is a shift of network defences toward a more comprehensive IT security model that allows organizations to restrict access controls to networks, applications, and environment without	discretion will be applied on assessment of the approach. • Application security is covered in 8.2.4 above. The Joint Standard applies to a variety of financial institution and depending on their nature, scale, complexity and risk profile, they may not be applying a Zero Trust Model. The Joint Standard covers the basic requirements for cybersecurity and resilience. • This is a minimum requirement and must be implemented by all financial institutions to which the Joint Standard applies. The second sentence has been deleted. In this regard, financial institutions must ensure that back-ups are secured, and they can use any modern mechanism to ensure the security and integrity of the back-up. –The offsite location includes cloud storage services. The Joint Standard has been amended to add (including cloud storage) after offsite location in the Joint Standard. • Institution specific or customer specific information will not be shared, it is more the modus operandi, trends, lessons, indicators of compromise, challenges etc. Financial institutions should engage in such arrangements to strengthen their cyber defence and resilience such as participation in industry CSIRT/ CERT, involved in committees such as CRS forums and industry association forums that deal with industry risk.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			sacrificing performance and user experience). It is suggested that the Authorities consider revising the requirement to "secure the access to the application" rather than securing the network • Paragraph 8.4.1 (d) Clarity is sought from the Authorities on: the requirement for backup media storage either offline or at an offsite location, and to what extent are organisations required to implement same. how this sub-section would apply to cloud storage services. Consideration should be given to the varying sizes and complexity of organisations within the financial sector. • Paragraph 8.5.2 (iii) We are not aware of mechanisms currently in place in order to facilitate adherence to the requirement. The industry would require support from the	• When the testing is not conducted by the financial institution, but the testing is done by the third-party service provider. • Environment refers to instances where the service is not managed by the institution but outsourced to 3rd party service provider. In this regard financial institutions can request reports such as ISAE 3402, audit reports, compliance reports, assessment of internal controls environment. • Noted, however only those deficiencies that are not resolved in a timely manner must be reported to the governing body and as such they become concerning for the purposes of risk. Therefore, since there is already a qualifier on what must be reported there is no need to include the word material. Cyber resilience capability includes people, process and technology.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			Authorities in order to comply with this requirement. We kindly request clarity if Authority's would support financial institutions to share cybersecurity information in order to comply with this requirement. • Paragraph 8.6.1 (b) The requirement around testing is not clear and we kindly request clarity on what is meant by "reliant on that party's information security control testing". We take note of the definition of "security controls" provided in the standard being a prevention, detection or response measure to reduce the likelihood or impact of a cyber incident. When would it be considered a financial institution is "reliant" on another party's information security control testing? • Paragraph 8.6.1 (a)(iv) Could the Authorities please clarify what is	

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			meant by “environments where a financial institution is unable to enforce its security policies”? Should an organisation not be able to enforce its security policies, then what do they need to test? It is proposed that this section is refined to be more specific regarding the intended requirement. • Paragraph 8.6.1 (c) It is our recommendation that requirement (c)(ii) needs to be more specific and clearly defined. It is our submission that the word “material” should be added, since it would be onerous and administratively intensive to escalate and report any testing results that identify security control deficiencies that cannot be remediated in a timely manner. We recommend amending it to read: "escalate and report to the governing	

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			body any results that identify material security control deficiencies that cannot be remediated in a timely manner." Paragraph 8.7.1 We require guidance on what is intent of cyber resilience capability. The current draft is not clear on whether this relates to a tool, people, policy, processes, or anything else	
99.	Financial Intermediaries Association of Southern Africa (FIA)	8.1.2(b) - Cyber Resilience	Does this include 3rd Party Service Providers?	Yes. 8.1.2(b) has been amended to clarify that it refers to 8.1.2(a) which includes the information etc that is managed by 3rd party service providers. Drafter to make reference to (a) in (b).
100.	Investec	8.1.2a	Typo – at the end it should be "service **providers**". It is also recommended that the requirement to identify business processes should not sit in the cybersecurity standard as this is not driven by cyber, but by the broader Operational Risk and Operational Resilience functions.	Noted. See revised Joint standard.
101.	Investec	8.1.2c	This statement reads as a broad risk function not specific to security, risk assessments are conducted business wide. It may be helpful to be specific and refer to technical risk assessments or security testing.	Noted. The Joint Standard has been amended to specify 'security' risk assessments.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
102.	Investec	8.1.2d	It is not practical to include "roles and responsibilities of staff managing information assets" as part of an inventory / CMDB.	Noted, the 'staff' element has been deleted. The paragraph now reads as follows: 8.1.2 (d) maintain an inventory of all its information assets which includes location, ownership, the roles and responsibilities of managing the information assets.
103.	Investec	8.1.3	Reviewing all information assets annually may be onerous, considering the definition. Propose taking a risk-based approach. It may also be useful to define what the expectation of the review is (e.g., access, if owners are correct, location, retention, disposal, etc.).	The Authorities agree that the review process might be onerous. However, based on the importance, a risk-based approach would not be sufficient as it may lead to longer term inaccuracies in the information assets inventory. This control requirement is to ensure that the inventory remain current, accurate and complete. The Authorities have revised paragraph 8.1.3 (now 8.1.2) to read: The inventory, referred to in paragraph 8.1.2(d) above must be updated when changes are required and reviewed regularly or at least biennially
104.	Standard Bank Group	8.2.1 Protection	A financial institution must implement appropriate and effective cyber resilience capabilities and cybersecurity practices to prevent, limit **and/or** contain the impact of a potential cyber event.	Noted. The Joint Standard has been amended accordingly.
105.	Bidvest Bank	8.2.2 (a) (v)	Clarity should be provided whether or not this requirement will be applicable to mobile devices accessing only email.	It does apply to mobile devices that are authorised to access the systems of the financial institutions.
106.	ASISA	8.2.2 (a)(v)	Not all users who access information assets will work from	Noted. The paragraph of the Joint Standard has been amended to include 'connections'

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			"devices that have been secured according to the financial institution's security standards". In those instances where they connect from unsecured devices, the mechanism that they use to connect to the information asset, provides the security, in other words no reliance is placed on the security of the device. Paragraph 8.2.2(a)(v) should be amended as follows: ------ "Ensure remote access to information assets is only allowed from devices that have ~~been secured according to the financial institution's security standards~~ **security posture commensurate to the risk associated with the information asset that is being accessed;** and	
107.	ASISA	8.2.2 (a)vi)	There is no definition of "strong authentication". It is suggested that the following definition is added to Paragraph 4 - Definitions and interpretation: ------ **Strong authentication is authentication requiring two or more factors of authentication to be true, these factors include**	The Authorities are of the view that there is no need to define strong authentication as this is a common term in cybersecurity and is an evolving concept.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			something I have, something I am, or something I know.	
108.	Investec	8.2.2(a)(vi)	Suggest being more specific about how "strong" authentication is quantified or evaluated to be sufficient.	See response to comment 106 above.
109.	Standard Bank Group	8.2.2 (a)(iv)	establish identity management and access control mechanisms to provide effective and consistent user administration, accountability, authentication, **and non-repudiation**.	Disagree, non-repudiation is not linked to identity and access and is rather linked to audit and integrity of data.
110.	Investec	8.2.2(a)(v)	Suggest rewording the phrase "only allowed from devices that have been secured according to the financial institution's security standards" to "devices and/or connections secured according to security standards". For example, a vendor device may not have security configurations or builds defined in the financial institutions' internal standards; but the manner in which they connect, authentication, and security restrictions would need to comply.	Noted. The paragraph has been amended to include connections. 'ensure remote access to information assets is only allowed from devices or through connections that have been secured according to the financial institution's security standards'; and
111.	Investec	8.2.3(a)(i)	Typo – at the end it should be "at rest **or in** use". Also, a financial institution should have the freedom to determine a risk-appropriate strategy, e.g., "prompting" rather than "preventing".	Noted. See revised Joint standard.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
112.	Standard Bank Group	8.2.3	Proposed addition to Data Security: limit sensitive data shared with 3rd parties or service providers to the minimum to achieve the business needs	Disagree, as this may then prohibit contracts that deal with sharing of sensitive data. It is the prerogative of each institution to ensure that when it shares sensitive data that it does so in the most secure manner and in consideration of applicable legislation.
113.	Standard Bank Group	8.2.3(a)(i)	develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, **and/or** transmission of its sensitive data whether in motion, at rest or in use.	Noted and amended accordingly.
114.	Purple Group Limited ("Purple Group")	8.2.3(a)(i)	Please advise as to how this requirement is complied with in the context of financial institutions sharing their data with third parties who are not required to comply with this Joint Standard? Does this requirement mean that the third parties financial institutions share their sensitive data with also need to comply with this provision? We respectfully submit that if this is the case, it will create additional challenges for the financial institutions when concluding agreements with third party service providers, and may require amendments to the existing agreements with third party service providers.	When dealing with third parties, financial institutions must ensure that such third parties have similar or the same level of security controls as the financial institution. If not, the financial institution will be more at risk to cybersecurity incident.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
115.	Purple Group Limited ("Purple Group")	8.2.3(a)(ii)	The system required to fulfil this requirement would be highly sophisticated and costly for a smaller financial institution who may have the systems to prevent but not detect especially across endpoint devices. Given the requirement in (iv) to further protect via encryption, would the Authority consider reducing this requirement to "prevention" only?	Please refer to comment 120 below for the amendment made to paragraph (iv). This Joint Standard contains minimum requirements for financial institution with regard to cybersecurity and cyber resilience.
116.	Purple Group Limited ("Purple Group")	8.2.3(a)(iii)	This provision is highly onerous on financial institutions who oftentimes make use of IT systems managed by third party providers due to lack of internal skills, capacity, and the fact that the systems required to do this are highly sophisticated. As we read it, this section requires the third party to comply with all the requirements in this Joint Standard – please clarify.	Noted. The Joint Standard has been amended as follows: ensure that IT systems managed by third party service providers are accorded the same level of protection and subject to the same security standards or are subject to protections and security standards that are commensurate to the sensitivity and criticality of the information being managed by the third party service provider;
117.	Investec	8.2.3(a)(iii)	Unsure about the practicality of this statement, especially how an institution will "ensure" on environments that they have no control over and will not have constant monitoring on. If this refers specifically to on-premises IT systems belonging to the financial institution but managed by a 3rd party, it should explicitly state this.	This is a minimum requirement of the Joint Standard as third parties have access to the information and systems of the financial institution. This can be established when the financial institution does its due diligence on a service provider before entering into a contract. Financial institutions should also consider the reports referred to in comment 118 below. Also note that sub-paragraph a(iii) has been amended.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
118.	Financial Intermediaries Association of Southern Africa (FIA)	8.2.3(a)(iii) –	In what form does 3rd party assurance need to be provided?	The form of assurance is not prescribed in this Joint Standard. Financial institutions can request reports such as ISAE 3402, audit reports, compliance reports, assessment of internal controls environment.
119.	Bidvest Bank	8.2.3(a)(iii)	Security standards for third party service providers might differ from that of the Bank, depending on the services provided to the Bank. It is recommended that the acceptable level of security standards be defined depending on the service/s provided to the Bank and the type of access between the Bank and the third-party service provider.	See response to comment 116 above.
120.	ASISA	8.2.3(a)(iii)	To ensure with a 100% certainty "that IT systems managed by third-party service providers are applying the same level of protection and subject to the same security standards" will be very onerous and costly on financial institutions. An element of reasonableness therefore needs to be factored into this statement. Paragraph 8.2.3(a)(iii) should be amended as follows: ------ "ensure, **as far as is reasonably possible**, that IT systems managed by third-party service providers are accorded the same level of protection and	Noted. See response to comment 116 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			subject to the same security standards."	
121.	Bidvest Bank	8.2.3(a)(iv)	It is recommended that this requirement be split between encryption on endpoints (laptops vs desktops) and the protection of sensitive data stored in systems. Clarity should be provided if the encryption of desktops is also a requirement as per the Joint Standard.	Noted. The Joint Standard has been amended as follows: ensure that sensitive information stored in systems and endpoint devices is encrypted and protected by access control mechanisms commensurate to the risk exposure.
122.	Standard Bank Group	8.2.3(a)(iv)	It may not always be feasible and practical to encrypt all sensitive data stored in systems and endpoints. However, there should be adequate security controls to protect sensitive data stored on systems and endpoints. The suggestion is: ensure that sensitive data stored in systems and endpoint devices is encrypted and protected by strong access control mechanisms, **based on classification and risk appetite**;	Noted. See response to comment 120 above.
123.	First rand Group	8.2.3(a)(iv)	Encryption is resource intensive and may not even on some legacy systems and databases without extensive upgrades and re-architecture. Encryption is also not the only mechanism	Noted. See response to comment 120 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			available to protect data in storage. Suggest that this section be split to deal with encryption on endpoints and that another section is created dealing with security requirements for systems that allows for the application of alternative mechanisms where encryption ifs not viable.	
124.	Silica Administration Services (Pty) ltd	8.2.3(a)(iv)	The requirement should rather state where feasible in accordance with the organisations risk appetite. To add "where practical and feasible"	Noted. See response to comment 120 above.
125.	Investec	8.2.3(a)(iv)	May not always be practical to encrypt data; other mechanisms should be allowed which afford sensitive data adequate protection against compromise and / or unauthorised access. Suggest including alternative controls such as masking, obfuscation, de-identifying system data.	Noted. See response to comment 120 above.
126.	Standard Bank Group	8.2.3(a)(v)	This statement excludes Bring Your Own Device. With increased work from home, the recommendation is to include a statement around BYOD having access to data with the correct levels of controls, eg strong	Only authorised devices that have security configuration similar to that of the financial institution can be used. BYOD will be permitted provided that it is authorised device. This is covered in the paragraph through the term authorised.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			authentication, device posturing, etc.	
127.	Investec	8.2.3(a)(vii)	Suggest changing "ensure that the use of sensitive production data in non- production environments must be **restricted"** from restricted to **limited**, as there may be an acceptable business need for this access.	There is a carve-out in the paragraph that can be followed in the instance suggested.
128.	Standard Bank Group	8.2.3(a)(viii)	ensure appropriate controls are implemented in **production and** non-production environments to manage the access and removal of sensitive data to prevent data leakages. Where possible, such data must be masked in the **production and** non-production environments;	Agree, the standard has been amended accordingly.
129.	Investec	8.2.3(a)(viii)	"Where possible, such data must be masked in the non-production environments" - suggest rewording to "Where possible, such data, **particularly PII data protected by POPIA**, must be **masked / deanonymized / obfuscated** in the non-production environments".	The information regulator will deal with these requirements.
130.	Bidvest Bank	8.2.3(a)(x)	This requirement should state that it is applicable to third party service providers. Copies of data should also be destroyed	Noted. The paragraph has been amended as follows: have an agreement in place for the secure return or transfer of data in instances where a contract, including a contract with a third-party service provider, is terminated and data has to be returned.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			by third party service providers once it has been returned.	If return is impossible, there must also be processes in place for the permanent deletion of copies of the financial institution's information as well as all the secure destruction of storage media containing the financial institution's information;
131.	First rand Group	8.2.3(a)(x)	Suggest adding context to this statement so that it is specific to use of 3rd parties. Furthermore, suggest that destruction should be required even when data has been returned. The current statement only requires destruction when data is not returned.	See response to comment 129 above.
132.	First rand Group	8.2.3(a)(x)	"have an agreement in place for the secure return or transfer of data in instances where the contract is terminated and data has to be returned, if return is impossible, **there should be processes in place for the secure destruction of storage media containing the financial institutions' information;"** Change highlighted section to read "there should be processes in place for the secure **permanent deletion of the financial institution's information and if this is not possible then** there must be secure destruction of storage media containing the financial institution's information**;**	See response to comment 129 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			Note that the contract should require destruction upon contract end or when legal requirement for retention has been met, irrespective of whether safe return is possible or not. The way it is currently worded, it implies that if the 3rd party can and does return the data safely then the 3rd party does not need to destroy the data.	
133.	Investec	8.2.3(a)(x)	The requirement is a little ambiguous in terms of scope – that is, whether it refers to staff, temporary workers, contractors, consultants, or third parties with whom a contract is in place.	Noted. See response to paragraph 129 above.
134.	Standard Bank Group	8.2.3(a)(x)	Please make explicit reference to a service provider or contractor in this case.	Noted. See comment 129 above.
135.	First rand Group	8.2.3(a)(xi)	This should be broader to take into account of users that are employees and do away with the need to enter into specific NDA's with employees as it could be become administratively challenging – suggest that the provision be amended to read "**have appropriate non-disclosure or confidentiality provisions included in the**	Noted. The paragraph has been amended to include 'appropriate' …provisions in the relevant agreements.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			relevant agreements with users"	
136.	Standard Bank Group	8.2.3(a)(xi)	have non-disclosure or confidentiality agreements in place with users **and service providers**.	Users include service providers as defined.
137.	Investec	8.2.3(a)(xi)	Suggest adding "with users and all third parties"	Users as defined in the Joint Standard includes third parties.
138.	Financial Intermediaries Association of Southern Africa (FIA)	8.2.4 – Application and security system	While we agree that security needs to be part of the design, it also needs to be pragmatic and not overly burdensome to the financial institution.	Noted. However, these are the minimum requirements of the Joint Standard.
139.	Bidvest Bank	8.2.4 (a) (iv)	Please clarify if Business and User Acceptance Testing (UAT) is sufficient or if specific security testing will be required for all changes. It is recommended that this requirement not be applicable to routine changes/maintenance and only appliable to major/material changes.	No, UAT will not focus on the security controls but rather on what the user needs to achieve with the application/system. Even a small change can cause an adverse impact. Because this relates to a critical system - even a small change must be reviewed.
140.	First rand Group	8.2.4 a (iv)	Reference is made here to "business critical applications". No definition is established for this.	It is up to the financial institution what is business critical seeing that there are many different types of financial institutions to which the Joint Standard applies.
141.	First rand Group	8.2.4 a (iv)	"ensure business critical applications are reviewed and tested to ensure that there is no adverse impact on operations or security when **changes** are made to such applications."	Disagree. Because it is business critical application any change has the potential to disrupt operations or security.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			We recommend the changes should not include routine changes e.g. capacity management, etc. but for material changes.	
142.	First rand Group	8.2.4 a (vi)	"encrypt **remote connections** to prevent data leakages through network sniffing and eavesdropping." Remote should be defined as external to the bank's network	The Authorities are of the view that 'remote' is an established term in the industry.
143.	Investec	8.2.4a(iv)	Suggest adjusting the wording to be clearer, e.g., "ensure changes to business critical applications are reviewed and tested to ensure that there is no adverse impact on operations or security of the applications."	Agreed. The paragraph has been amended and now reads: ensure that changes to business critical applications are reviewed and tested to ensure that there are no adverse impact on operations or security. .
144.	Investec	8.2.5	Suggest adding a requirement to review firewall rules on a periodic basis and adding a requirement to test network perimeter controls and posture at least annually by certified professionals.	Noted. We have added a requirement to review firewall rules on a periodic basis as well as to test network perimeter controls and posture at least annually.
145.	ASISA	8.2.5 (a)(iv)	The reference to network access control could be confused with a general industry term NAC. Considering the wide adoption of the Zero Trust model across the cybersecurity industry where there is a shift of network defences toward a more	Noted. The Authorities are of the view that controls are wider than protocols. However, the latter part regarding the change from control 'rules in the network devices' to 'access mechanisms' has been amended in accordance with the suggestion.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			comprehensive IT security model that allows organizations to restrict access controls to networks, applications, and environment without sacrificing performance and user experience. Paragraph 8.2.5(a)(iv) should be amended as follows: --- "implement network access ~~controls~~ **protocols** to detect and prevent unauthorised devices from connecting to its network. Network access ~~control rules in network devices~~ **mechanisms** must be reviewed on a regular basis to ensure they are kept up to date;"	
146.	Bidvest Bank	8.2.5 (v)	The requirement is vague and clarity is required – does the requirement entail the Bank implementing controls to prevent some users from accessing the internet from their endpoint devices?	Noted. The word 'consider' has been removed and the paragraph has been amended to read: 'isolate internet web browsing activities from sensitive IT systems ~~endpoint devices~~ through the use of physical or logical segregation, or implement equivalent controls, to reduce exposure of its IT systems to cyber-attacks; and .
147.	First rand Group	8.2.5 a (v)	Remove this section as it comes across as a guidance rather than expectation and is ambiguous	See comment 145 above.
148.	Standard Bank Group	8.2.5 Network Security (a) (v)	consider isolating internet web browsing activities from its endpoint devices through the	See comment 145 above

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			use of physical or logical segregation, or implement equivalent controls, to reduce exposure of its IT systems to cyber-attacks; and This is worded as a non-mandatory control (consider). Should this be in a standard if it is not mandatory?	
149.	Standard Bank Group	8.2.5 Network Security(a) A financial institution must –	Proposed addition: ensure that all remote user access infrastructure is protected from compromise and denial of service attacks ensure that all client facing systems are protected from compromise and denial of service attacks, based on criticality	Noted, however, the suggestions have been broadly covered under Identity and access management (paragraph 8.2.2 of the Joint Standard) and Application and System security (paragraph 8.2.4) and Data security (8.2.3).
150.	ASISA	8.2.5(a(v)	Confirmation is required that this refers to normal network security and browsing proxies, limiting access to what can be seen on the internet.	No. The paragraph has been amended to make the intention clear. See response to comment 145 above.
151.	Purple Group Limited (“Purple Group”)	8.2.5(a)(ii)	Would this requirement be applicable to a third party who manages and accesses a financial institutions data? We respectfully submit that, if so, create additional challenges for the financial institutions when concluding agreements with third party service providers, and	Yes. Please consider 8.2.3(a)(iii) above. The financial institution is ultimately responsible even when third parties are providing services.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			may require amendments to the existing agreements with third party service providers.	
152.	Purple Group Limited ("Purple Group")	8.2.5(a)(iv)	Please advise what 'regular' review means in respect of this requirement i.e. how often would a financial institution need to review their network access control rules in network devices? This may be an onerous requirement for smaller financial institutions who do not have the employees with the necessary skills and capacity which means that the financial institution will have to outsource this requirement and as a possible consequence, financial institutions may increase their fees to cover the additional overhead costs and this will negatively impact the client.	Noted. The paragraph has been amended to add, but at 'least annually'.
153.	Investec	8.2.5(v)	We are happy with this statement provided it starts with 'Consider…' because there are other ways to mitigate this risk depending on the complexity of the environment. Also, clarify what is being referred to here (e.g., dirty browser") as the word "consider" implies that it is not a mandatory minimum control.	"Consider' has been removed as this paragraph communication a requirement. The point is to segregate your network in order to reduce the attack surface. See response to comment 145 above.
154.	Silica Administration Services (Pty) ltd	8.2.5(vi)	To add: "where possible"	Disagree – this is a minimum requirement.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
155.	Financial Intermediaries Association of Southern Africa (FIA)	8.2.6 - Cryptography	This appears to be a very onerous provision, especially for smaller Category II FSPs. Proportionality is required here.	Noted. the Paragraph has been amended to say "where a financial institution uses cryptography it must…."
156.	Purple Group Limited ("Purple Group")	8.2.6(a)(i)	Please provide guidance on which data must be encrypted and what standards of encryption are applicable to this provision.	This depends on data/information sensitivity classification. Financial institution must follow best practice and the Authorities do not prescribe a specific frameworks in this regard.
157.	ASISA	8.2.6.(a)(i)	This requirement is applicable to banks, but not necessarily to all financial institutions where the use of cryptography is built into systems and does not require all these components. Paragraph 8.2.6(a)(i) should be amended as follows: ------- **"where encryption keys are managed, ensure that the practices are guided by clear** ~~establish~~ cryptographic key management policies, standards and procedures covering key generation, distribution, installation, renewal, revocation, recovery and expiry; **"**	Noted. See response to comment 154 above.
158.	Purple Group Limited ("Purple Group")	8.2.6.(a)(ii)	Please provide guidance on which international standards are applicable in respect of the cryptographic algorithms.	Please note that this section only applies to financial institutions that use cryptographic encryption. Please see response to comment 154 above.
159.	Investec	8.2.6a(vii)	It may not be practical for all cryptographic algorithms / keys to be rigorously tested; this	Disagree. It is necessary for the financial institution to test the algorithms in terms of compatibility with

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			should not be a mandatory requirement given that algorithms from well-established standards must be used as per 8.2.6a(ii). There should not be any additional expectation for an institution to do additional testing and vetting if well-established and industry standard algorithms are adopted.	the system or whether it is achieving what was intended.
160.	First rand Group	8.2.7 (ii)	The annual minimum requirement for training might not be appropriate. E.g. if an organisation has developed a library of training material that is refreshed with new modules that are rolled-out to all / new employees. So, there is no requirement for employees to reperform a learning module annually but for all employees to have completed all new modules.	Noted. The paragraph has updated. Refresher training is done at least annually and training on new content is done regularly in consideration of the evolving risks..
161.	A2X Markets	8.3.1 (d)	A dedicated Security Operations Centre is not practical or required for A2X given the size of the company / IT infrastructure. Provided that the end objective is achieved and A2X can illustrate that, that should suffice.	Noted, however, the Joint Standard provides for minimum requirements for financial institution. This paragraph provides an option to establish a dedicated security operational centre **or** acquire managed security services in order to facilitate continuous monitoring and analysis of cyber events as well as prompt detection and response to cyber incidents - to cater for the nature, scale, complexity and risk profile of a financial institution. The paragraph has also been amended – see response to comment 163 below.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
162.	China Construction Bank Corporation Johannesburg Branch	8.3.1 Detection – D	States a financial institution must establish a security operations centre – for banks who are smaller in size and complexity and do not have the resources / budget / infrastructure to support a security operations centre, however are supported by a parent organisation who does have this infrastructure and supports the branch – is this sufficient to meet the requirement? Or should the bank establish their own SOC or acquire third party SOC managed services from a local party?	See response to comment 160 above.
163.	First rand Group	8.3.1 f	Suggest that "establish a process to collect, review and retain IT system logs to facilitate security monitoring operations. These logs must be protected against unauthorised access" be revised as "establish a process to collect, review and retain **relevant** IT system logs to facilitate security monitoring operations. These logs must be protected against unauthorised access" to avoid the unintended and impractical	The requirement is not that a financial institution retains all logs but only logs relevant to security event monitoring. The retention of logs must be done in accordance with the retention policy of the financial institution.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			expectation that all systems are logged and all logs are retained	
164.	Investec	8.3.1(d)	Not all organisations can establish or afford a SOC. A good monitoring and incident response team can be just as effective. Suggest rewording to "Establish a security operations centre / monitoring and incident response team, or acquire managed security services".	Noted. The paragraph has been amended to: establish a security monitoring capabilities, such as a security operations centre (or similar), or acquire managed security services, in order to facilitate continuous monitoring and analysis of cyber events as well as prompt detection and response to cyber incidents;
165.	Financial Intermediaries Association of Southern Africa (FIA)	8.3.1(d) - Detection - Security Operation Centre	This appears to be a very onerous provision, especially for smaller Category II FSPs. Proportionality is required here.	See response to comments 160 and 163 above.
166.	Investec	8.3.1a - 8.3.1c	Consider combining these three points as they are very similar; both refer to the ability to monitor an IT environment and systems to be able to detect and swiftly respond to potential or actual cyberattacks / compromise. In addition, "exercises" at the end of the sentence is vague – it is unclear what is being referred to. Clarity is sought.	Noted. The Joint Standard has been amended as follows : A financial institution must maintain effective cyber resilience capabilities to– ~~(a) maintain effective cyber resilience capability to recognise signs of a potential cyber incident, or detect that an actual compromise has taken place;~~ (b) ~~must monitor IT systems activities to~~ systematically monitor and detect actual or attempted attacks on IT systems and business services as well as effectively respond to attacks; (c) ~~establish systematic monitoring processes to rapidly detect cyber incidents~~ (d) periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, and audits 8.3.2 A financial must in implementing the requirements stated in paragraph 3.1 above, consider (e) to (i) follows.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
				Noted "exercise' has been removed as it is covered in 'testing'.
167.	Investec	8.3.1g	Suggest removing reference to "performance" as this is beyond the scope of a cyber standard; it should only refer to monitoring of potential security issues. Statement should explicitly indicate **security events and alerts**.	Noted. 'Performance' has been removed from the paragraph and the word 'security' has been placed before events and alerts..
168.	ASISA	8.3.2 (a)(iv)	The operational and financial impact of encrypting all sensitive data stored in systems will be significant. This requirement does not take compensating controls into account. Encryption should be used where it makes sense. Paragraph 8.2.3(a)(iv) should be amended as follows: --- " ensure that sensitive data stored in systems and endpoint devices ~~is encrypted and~~ **are protected by** ~~strong~~ **robust** access control mechanisms**; encryption should be used to reduce the risk of data interception, loss or theft"**	8.2.3(a)(iv) - Noted. The Joint Standard has been amended as follows: ensure that sensitive information stored in systems and endpoint devices is encrypted and protected by access control mechanisms commensurate to the risk exposure;
169.	Bidvest Bank	8.4.1 (d)	Please clarify if this requirement is applicable to cloud service providers with regards to offline/offsite backups.	The offsite location includes cloud storage services. The Joint Standard has been amended to include cloud storage.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
170.	Allan Gray	8.4.1 paragraph (d)	With the advent of cloud it could be difficult to bring all the data back to physical tapes- and then store offsite. Is a read only/ immutable archive acceptable? This would be a cloud storage option	See response to comment 168 above.
171.	Purple Group Limited ("Purple Group")	8.4.1(a)	Financial institutions may not have the employees with the necessary skills in-house. This will require that a financial institution outsource this function and this will have additional costs as a consequence which may negatively impact the customers as the financial institution will likely increase customer fees to cover the increased costs which adversely impacts customers.	This Joint Standard prescribes minimum requirements for financial institutions on Cybersecurity and Cyber resilience. Due to the highly digitalised operations of financial institutions these minimum requirements must be complied with. The impact on a financial institution is dire when a cyber incident occurs both to the financial soundness of the financial institution and to financial customers.
172.	ASISA	8.4.1(d)	Data storage requirements should also apply to cloud storage services and consideration should be given to the varying sizes and complexity of organisations within the financial sector. Paragraph 8.4.1(d) should be amended as follows: "ensure any sensitive data stored in the backup media is secured ~~(e.g., encrypted). Backup media must be stored offline or at an offsite location~~**; in an immutable manner,**	See response to comment 168 above. This is a minimum requirement of the Joint Standard in relation to sensitive information.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			irrespective of the location; and"	
173.	Investec	8.4.1(d)	May not always be practical considering implications on recovery and restoration time frames.	This is a minimum requirement of the Joint Standard in relation to sensitive information. Also, see response to comment 168 above.
174.	ENSAfrica	**8.4.1(d)** A financial institution must ensure any sensitive data stored in the backup media is secured (e.g. encrypted). Backup media must be stored offline or at an offsite location;	In our experience many financial institutions have embarked on a cloud strategy which would include the storing of sensitive data and backup date being located in the cloud. We request the Authorities to consider and clarify to what extent this requirement may be extended to storage in the cloud.	See response to comment 168 above.
175.	Rand Mutual Assurance	8.4.1(d) – Backup must be stored at an offsite location	Can we include clarity of whether such offsite locations must be local, or does it include international? (Microsoft backup storage facilities are located across international borders)	See response to comment 168 above.
176.	ENSAfrica	**8.4.1(e)** A financial institution must implement a clear communication strategy to financial customers impacted by cyber-attacks including details on any recourse available to financial customers.	Dealing with and responding to cyber-attacks is complicated and not a one-size-fits-all approach. The Authorities should consider engaging with the relevant structures established by the Cybercrimes Act who are tasked with assisting victims of cybercrimes. The Authorities should thereafter consider how this can be consolidated with the	This is a minimum requirement that requires the financial institution to communicate to financial customers when they have been impacted. It is important, from a conduct and fair treatment perspective of clients, that they be informed about the possible impact. Although the Authorities participate in various fora dealing with cybersecurity issues, participating in other fora will be assessed based on all the relevant policy considerations.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			obligation imposed by this section 8.4.1.(e).	
177.	BASA	8.4.1. d	**Clarify** what is meant by "backup media must be stored offline" and, how does this relate to cloud backup solutions provided. **Clarify** if offline backups are required where applications have high availability. Where cloud providers are used to providing infrastructure, there is limited ability to store backups offline, or in an air-gapped environment. **Recommend** allowing organisations to use more modern mechanisms to protect backups against ransomware threats. Offsite or offline storage is not always practical. There are other options such as cloud storage service where data can be replicated, but versions of data records are kept for a period of time before they are rotated/destroyed. Offline is not practical in many situations. Some entities are developing the use of immutable backups which do not require offline storage. Agree that backups are important and that firms review their capabilities in light of growing threats but given the	See response to comment 168 above. Paragraph 8.4.1 (c) has been amended to include testing of back-ups as follow: establish data backup strategy, and develop a plan to perform regular backups a**nd testing** so that IT systems and data can be recovered in the event of a ~~disruption~~ **cyber incident** or when data is corrupted or deleted. . The paragraph has been amended to include a cyber-incident which will cover ransomware.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			pace of change in both defence and threats, prescribing specific solutions is unlikely to give firms the flexibility they need to stay up to date with the threats they face. **Recommend** the testing of backups against a ransomware event be mandatory. One must consider a scenario where information system configuration, and data are lost across primary and backup sites, and one would need to restore from offline or version-controlled images. **Recommend** mandatory testing includes a focus on system binaries and configurations as well, and not just databases. **Recommend** that air-gapped backups be a separate requirement and be done on a criticality/prioritization basis. Normal backups could inter alia also refer to replication i.e., making a copy of data in an online state.	
178.	Standard Bank Group	8.4.2 Incident response and management	Proposed addition: Incident response plans should be simulated and tested annually to ensure that they meet the latest threats	Noted. The paragraph has been amended to add: (iv) the cyber incident response and management plan must be tested to ensure that meet the latest cyber threats.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
179.	Investec	8.4.2a(ii)	Propose splitting this into two separate requirements. That is, have a separate point in the standard for the following: "Information from cyber intelligence and lessons learnt from cyber incidents must be used to enhance the existing security controls or improve the cyber incident response and management plan."	Noted. The paragraph has been split into (ii) and (iii) accordingly.
180.	BASA	8.5.2	Threat intelligence and information sharing (a) A financial institution must – (i) establish a process to collect and analyse cyber-related information for its relevance and potential impact to the business and IT environment in order to maintain good cyber situational awareness. (ii) implement cyber intelligence monitoring capabilities; and (iii) actively participate in cyber threat information-sharing arrangements with trusted external and internal parties: (aa) to share reliable, actionable cybersecurity information regarding threats, vulnerabilities, incidents to enhance defences; and (bb) to receive timely and actionable cyber threat information.	Financial institution must when sharing threat intelligence and other information related to cybersecurity must comply with other legislation retaining to sharing of information etc. as well as their own policies on data sovereignty.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			Clarify if data sovereignty considerations been factored in for financial institutions with a global presence. **Clarify** how financial services institutions can ensure personal identifiable information is not shared as part of threat intelligence and information sharing.	
181.	Financial Intermediaries Association of Southern Africa (FIA)	8.5.2 - Situational Awareness - Threat Intelligence	Additional guidance is required from the Regulators on exactly what would be required.	Financial institutions must follow best practice. specific or customer specific information will not be shared, it is more the modus operandi, trends, lessons, indicators of compromise, challenges etc. Financial institutions should engage in such arrangements to strengthen their cyber defence and resilience such as participation in industry CSIRT/ CERT, involved in committees such as CRS forums and industry association forums that deal with industry risks. A financial institution must apply the principles regarding Threat Intelligence as commensurate to the nature, scale, size and complexity of its operations.
182.	BASA	8.5.2 (iii)	**Recommend** deleting "Must….actively participate in cyber threat information-sharing arrangements with trusted external and internal parties…." This is something that cannot be prescribed as it is subjective and difficult to measure. **Replace** must with recommend. **Recommend the** above is also applicable for the subpoints (aa) and (bb).	Institution specific or customer specific information will not be shared, it is more the modus operandi, trends, lessons, indicators of compromise, challenges etc. Financial institutions should engage in such arrangements to strengthen their cyber defence and resilience such as participation in industry CSIRT/ CERT, involved in committees such as CRS forums and industry association forums that deal with industry risk. The Joint Standard has been amended – to remove 'Actively' and internal parties

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			The voluntary element of information sharing is vital and must be protected. If information sharing were to become mandatory it would become difficult to maintain trust and the quality of information shared may decline as a result. In addition, if financial entities are forced to participate and share information, there is a risk that information-sharing groups will be flooded with low-quality intelligence, distracting resources from analysing higher-quality information shared voluntarily.	
183.	First rand Group	8.5.2 (iii)	Must …."actively participate in cyber threat information-sharing arrangements with trusted external and internal parties…." is something that cannot be prescribed as it is subjective and impossible to measure…suggest this is removed Same applies to the subpoints (aa) and (bb)	See comment 181 above.
184.	China Construction Bank Corporation Johannesburg Branch	8.5.2 Situational Awareness – iii	States active participation in cyber-threat sharing arrangements with trusted external and internal parties – are there financial industry forums where banks can share	See comment 181 above

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			knowledge and experience? Currently most banks in the industry are reluctant to share cyber-related event information that could be beneficial to other banks.	
185.	Purple Group Limited ("Purple Group")	8.5.2(a)(i)	Financial institutions may not have the employees with the necessary skills in-house. This will require that a financial institution outsource this function or hire additional resources and this will have additional costs as a consequence which may negatively impact the customers as the financial institution will likely increase customer fees to cover the increased overheads which adversely impacts customers.	This Joint Standard prescribes minimum requirements for financial institutions on cybersecurity and cyber resilience . Due to the highly digitalised operations of financial institutions these minimum requirements must be complied with. The impact on a financial institution is dire when a cyber incident occurs both to the financial soundness of the financial institution and to financial customers.
186.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	8.5.2(iii) & 8.6.1(b) & 8.6.1(c)	8.5.2 (iii) Situational awareness We are not aware of mechanisms currently in place in order to facilitate adherence to the requirement. We recall meetings with some of the regulatory bodies where it was discussed that financial services companies could leverage off the information and threat sharing platforms in place between the banks. There were further discussions around creating a separate platform for financial services companies. We are	Insurers should approach the industry bodies to facilitate such information sharing platforms on cybersecurity and cyber resilience.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			however not aware of these plans being executed and OUTsurance is currently not part of any such forums. As a financial institution it is our submission that financial institutions would require support from the Authorities in order to comply with this requirement. We kindly request clarity if Authority's would support financial institutions to share cybersecurity information in order to comply with this requirement. 8.6.1 (b) Testing The requirement around testing is not clear and we kindly request clarity on what is meant by "reliant on that party's information security control testing". We take note of the definition of "security controls" provided in the standard being a prevention, detection or response measure to reduce the likelihood or impact of a cyber incident. When would it be considered a financial institution is "reliant" on another party's information security control testing? 8.6.1 (c) Testing	When you have outsourced the function or you cannot conduct the security testing yourself. Noted, however only those deficiencies that are not resolved in a timely manner must be reported to the governing body and as such they become concerning for the purposes of risk. Therefore, since there is already a qualifier on what must be reported there is no need to include the word material.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			It is our recommendation that requirement (c)(ii) needs to be more specific and clearly defined. It is our submission that the word “material” should be added, since it would be onerous and administratively intensive to escalate and report any testing results that identify security control deficiencies that cannot be remediated in a timely manner. We recommend amending it to read: "escalate and report to the governing body any results that identify material security control deficiencies that cannot be remediated in a timely manner."	
187.	SA Home Loans	8.6.1	The following clause “(a)(i) the rate at which the vulnerabilities and threats change;” is quite broad as these could change daily. It may be more practical to narrow this timeframe (e.g. monthly/quarterly, etc) as institutions may not have the expertise available as defined in 8.6.1(c)(i)and would need to purchase specialised services as a significant cost.	The Authorities are unable to prescribe a time period for this requirement as it is necessary to continuously test the security controls in place as threats evolve.
188.	Financial Intermediaries Association of Southern Africa (FIA)	8.6.1 – Testing	Additional guidance is required from the Regulators on exactly what would be required, i.e. what form and frequency etc?	See response to comment 186 above. The testing must be commensurate to the nature, scale, complexity, risk profile of a financial institution.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
189.	Bidvest Bank	8.6.1 (b)	Clarity to be obtained whether or not the Bank can obtain assurance letters from its third party service providers or their certification of compliance to acceptable and recognised international frameworks or standards such as PCI, ISO, ISAE3402.	Yes, these letters or certifications will be acceptable to the Authorities. The paragraph has been amended in the following manner: Where a financial institution's information assets are managed by a third-party service provider, and a financial institution is reliant on that party's information security control testing, the **financial** institution **must be satisfied** that **the** nature and frequency of testing of controls in respect of those information assets is commensurate with sub-paragraphs (i) to (v) above. Ultimately overall responsibility and accountability remains with the entity.
190.	BASA	8.6.1 a	**Correct** typo error in "teffectiveness."	Noted and amended.
191.	First rand Group	8.6.1 a	Correct typo error in "teffectiveness".	Noted and amended.
192.	First rand Group	8.6.1 b	The standard should make provision for the financial institution to satisfy itself on the control environment of the third party service provider through an assurance letter from their independent assurance provider or be able to rely on the third party's certification of compliance to an acceptable and recognised international framework / standard (e.g. NIST, ISO, etc) as many of the large IT (including cloud) third party service providers will not provide detailed reports on the outcomes of their control testing	See response to comment 188 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			or remediation plans and will also not allow a financial institution (as a client) to test their controls or appoint an independent assurance provider to do so on the financial institution's behalf.	
193.	Silica Administration Services (Pty) ltd	8.6.1(a)(i)	This is not feasible as the rate at which vulnerabilities and threats change are dynamic. An organisation must react to vulnerabilities and threats 'as and when'.	The Joint Standard in this paragraph is specifically referring to the testing of security controls and not the reaction to vulnerabilities. The testing must be commensurate to the nature, scale, complexity and risk profile of a financial institution.
194.	ENSAfrica	**8.6.1(a)(iv)** A financial institution must test all elements of its cyber resilience capacity and security controls to determine the overall effectiveness, whether it is implemented correctly, operating as intended and producing desired outcomes. The nature and frequency of the testing must be commensurate with the risks associated with exposure to environments where a financial institution is unable to enforce its security policies;	We request the Authorities to please clarify the phrase "environments where a financial institution is unable to enforce its security policies"? This section seems to suggest that in instances where a financial institution is not in control of the environment, such as where a third party service provider is used. Is the intention then that the financial institution must impose contractual provisions on such third party service provider to conduct such testing and report back to the financial institution on a regular basis? This seems to be suggested by 5.2.3. If this is not the case, we suggest this be further clarified, alternatively, this section be	Yes, the requirement includes third party service providers. Also see 8.6.1(b) which relates specifically to third party service providers.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			expanded to include the above position.	
195.	Purple Group Limited ("Purple Group")	8.6.1(c)(i)	Financial institutions may not have the employees with the necessary skills in-house. This will require that a financial institution outsource this function and this will have additional costs as a consequence which may negatively impact the customers as the financial institution will likely increase customer fees to cover the increased overheads which adversely impacts customers.	This Joint Standard prescribes minimum requirements for financial institutions on cybersecurity and cyber resilience. Due to the highly digitalised operations of financial institutions these minimum requirements must be complied with. The impact on a financial institution is dire when a cyber incident occurs both to the financial soundness of the financial institution and to financial customers.
196.	BASA	8.6.1. b	**Clarify** the definition of Information Assets will require additional clarity to establish liability. **Clarify** if this supersedes GN5/18 requirements. **Recommend** that the standard make provision for the financial institution to satisfy itself on the control environment of the third-party service provider through an assurance letter from their independent assurance provider or be able to rely on the third party's certification of compliance to an acceptable and recognised international framework / standard (e.g., NIST, ISO, etc). A significant number of the large IT (including	There is a definition for information assets. The definition has also been amended to exclude paper-based information. The risk associated with the information assets rests with the financial institution itself whether it is stored within the institution or with a third-party service provider. The requirements in the Joint Standard supercedes any Guidance Notes issued in terms of the Banks Act. This Joint Standard does not contradict the provisions of the Guidance Note. Banks must however still follow the Guidance Note and apply the higher standards of the Joint Standard where necessary. The paragraph has been amended. See response to comment 188 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			cloud) third party service providers will not provide detailed reports on the outcomes of their control testing or remediation plans and will also not allow a financial institution (as a client) to assess their controls or appoint an independent assurance provider to do so on the financial institution's behalf.	
197.	Silica Administration Services (Pty) ltd	8.6.1©(ii)	Consider adding that "timely will depend on the organisation's risk profile/appetite".	The Authorities have not specified what is meant by timely and this will be assessed during supervision.
198.	Investec	8.6.1a	Typo – should be "determine the overall **effectiveness**". Propose change from "it is implemented" to "they are implemented" as we are referring to numerous controls	Noted and amended.
199.	Silica Administration Services (Pty) ltd	8.6.2(a)(i)	Consider adding that "timely will depend on the organisation's risk profile/appetite".	The Joint Standard applies to different financial institutions. The Authorities have not defined 'timely' and will assess this during supervision.
200.	BASA	8.6.2. a	**Clarify** if "risk arising" means the closing of the vulnerability or the implementation of compensating controls or both.	The paragraph has been amended to eliminate any confusion as follows: establish a process to conduct regular vulnerability assessments on its IT systems to identify security vulnerabilities and ensure ~~risk arising from these~~ **that** vulnerabilities are addressed in a timely manner; and
201.	SA Home Loans	8.6.3	Comprehensive penetration testing is an expensive exercise for most institutions. When is the proposed commencement date	The commencement date is approximately 12 months after publication.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			so that institutions can set appropriate budgets?	
202.	Financial Intermediaries Association of Southern Africa (FIA)	8.6.3 – Penetration Testing	We request that a proportional approach be applied here. For smaller Category II FSPs, these requirements are particularly onerous.	In practice, the Authorities will adopt a risk-based approach to supervision of the Joint Standard, which means that focus and regulatory interventions are commensurate to the risks and impact that entities pose to the financial sector. The Authorities may also support compliance with the Standard, helping especially smaller entities to understand their regulatory obligations, by providing additional regulatory guidance through for example a Guidance Notice. The proposed requirements facilitate proportional application of the Standard and provides that the requirements must be implemented in accordance with the risk appetite, nature, size and complexity of a financial institution. If there are still instances where a specific requirement is too onerous on a small financial institution despite application of the principle of proportionality, an exemption from a specific requirement of the Standard may be considered,
203.	Bidvest Bank	8.6.3 (a) (i)	The requirement is too prescriptive – It is recommended that reference to black box, grey box and white box testing be deleted as this will have a significant financial impact on the Bank.	Noted. The paragraph has been amended to remove the requirement for black/white/grey box testing to be done but to include an enabling provision to the effect that the Authorities may, based on the nature, scale, complexity and risk profile of the financial institution specify that a black box, white box, grey box testing or a combination thereof be conducted.
204.	BASA	8.6.3 (a) iii	“conduct penetration testing to validate the adequacy of the security controls for IT systems and information assets that are	Noted. The paragraph has been amended to make this requirement clear. Noted. The paragraph has been amended to remove the requirement for black/white/grey box testing to be done but to

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			directly accessible from the internet**, at least annually or whenever such IT systems and information assets undergo major changes or updates**." **Recommend** enhancing the highlighted wording to read as follows: "whenever such IT systems and information assets undergo major changes or updates or at least annually." Tools other than penetration testing may be used at large financial entities to achieve this result, such as automated scanning. **Recommend** that the text be updated to allow for the use of new and evolving tools.	include an enabling provision to the effect that the Authorities may, based on the nature, scale, complexity and risk profile of the financial institution specify that a black box, white box, grey box testing or a combination thereof.
205.	First rand Group	8.6.3 (a) iii	This is unclear – is there a requirement that each one of the systems that has internet access should be tested annually in relation to a cyber vulnerability. The practicality of such a requirement should be revisited.	All internet-facing systems must be tested annually.
206.	First rand Group	8.6.3 (a) iii	"conduct penetration testing to validate the adequacy of the security controls for IT systems and information assets that are directly accessible from the internet**, at least annually or whenever such IT systems and information assets**	See response to comment 203 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			undergo major changes or updates." Highlighted wording doesn't make sense – it should read as follows: "whenever such IT systems and information assets undergo major changes or updates or at least annually".	
207.	A2X Markets	8.6.3 (a)(i)	We do annual testing but this requirement will increase the scope of the testing significantly and would be prohibitively expensive. Provided that the end objective is achieved and A2X can illustrate that, that should suffice.	See response to comment 202 above.
208.	BASA	8.6.3 a (i)	**Recommend** deleting "A combination of black box, grey box and white box testing must be conducted for IT systems and information assets" as it is too prescriptive. This Joint Statement place a heavy emphasis on penetration testing. While testing can yield benefits for a financial entity's ability to monitor its cyber risk, testing is only one of many controls that entities use, and it is not always the most appropriate due to the complexity, risks, and costs of conducting such testing.	See response to comment 202 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
209.	Just Retirement Life (South Africa)	8.6.3 Penetration testing – (a)(i)	"A combination of black box, grey box and white box testing must be conducted for IT systems and information assets" - this will result in additional costs and it will be useful to get some guidelines on the frequency of the different types of testing required (i.e. black, grey and white box).	See response to comment 202 above
210.	ASISA	8.6.3(a)(i)	Financial institutions cannot be forced to use all three types of testing, it depends on the maturity of the company and the risk associated with the system. Paragraph 8.6.3(a)(i) should be amended as follows: --- "carry out penetration testing to obtain an in-depth evaluation of its cybersecurity defences. A combination of black box, grey box and white box testing ~~must~~ **could** be conducted for IT systems and information assets;"	See response to comment 202 above
211.	Purple Group Limited ("Purple Group")	8.6.3(a)(ii)	Any one of these tests are very costly, financial institutions will have to pay for these tests and it is impractical and expensive to execute a combination of these tests simultaneously. Financial institutions will need adequate time between each test spread over a calendar year or calendar	See response to comment 202 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			years. We respectfully submit that the Authority consider that a financial institution must do one of these tests annually.	
212.	BASA	8.6.3.	**Clarify** the details of this requirement since this will have a direct impact on testing capabilities and capacity as well as budgets.	See response to comment 202 above.
213.	BASA	8.6.3. a (iii)	**Clarify** is this limited to pre-go live and production assurance. **Clarify** is there a requirement that each one of the systems, which have internet access, must be assessed annually for cyber vulnerability. **Recommend** that the frequency of testing be based on criticality and impact.	This relates to the production environment. Yes. Kindly see 8.6.3 (a)(ii) which says - (ii) ensure that the frequency of penetration testing is determined based on factors such criticality and exposure to cyber risks.
214.	Investec	8.6.3a(i)	As per comment #3, suggest removing references to “black / grey / white” box testing; it should simply refer to penetration testing as a requirement for clarity and simplicity. Also suggest adding that “critical systems be given priority, in particular those that are exposed to the Internet or interfacing with the internet”.	See response to comment 202 above. Refer to 8.6.3 (a)(ii) which refers to the frequency of the testing based on criticality and exposure to cyber risk. Also refer to 8.6.3(a)(iii) which deals with internet facing system.
215.	A2X Markets	8.6.4	Simulation exercises would not be practical nor commensurate with the size and complexity of the A2X business.	This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect, detect, respond and recovery from cyber incidents. The impact of a

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
				cyber event has disastrous impact on the financial institution and financial customers.
216.	Financial Intermediaries Association of Southern Africa (FIA)	8.6.4 – Simulations	We request that a proportional approach be applied here. For smaller Category II FSPs, these requirements are particularly onerous.	See response to comment 201 above.
217.	Purple Group Limited ("Purple Group")	8.6.4(i)	Please provide guidance on how regularly this must be done. The financial institution will have to dedicate resources to deal with the results of these tests and the environment must be duplicated for these tests which are costly. The increased costs will negatively impact the financial institution and will require additional resources. Financial institutions may be forced to increase their fees paid by clients.	Regular must be interpreted in this paragraph in accordance with the nature, scale, complexity and risk profile of the financial institution. This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect , detect, respond and recovery from cyber incidents. The impact of a cyber incidents has disastrous impact on the financial institution and financial customers.
218.	SA Home Loans	8.6.5	Is Application Security Testing limited to applications exposed to the Internet or all applications used/developed within an institution?	Noted. The paragraph has been amended as follows: A financial institution must – (i) carry out testing of security functionality on **web-based and critical** applications during the implementation in a robust manner to ensure that they satisfy business policies or rules of the financial institution as well as regulatory and legal requirements.
219.	Financial Intermediaries Association of Southern Africa (FIA)	8.6.5 – Application Security Testing	We request that a proportional approach be applied here. For smaller Category II FSPs, these requirements are particularly onerous.	Noted. The paragraph has been amended as follows: A financial institution must – (i) carry out testing of security functionality on **web-based and critical applications** during the implementation in a robust manner to ensure that

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
				they satisfy business policies or rules of the financial institution as well as regulatory and legal requirements. Also see response to comment 201 above.
220.	Standard Bank Group	8.6.5 Application security testing a (iii)	establish a policy and procedure on the use **and update of** third-party and open-source software codes to ensure these codes are subject to review and testing before they are integrated into a financial institution's software.	Noted. The Joint Standard Bank has been updated accordingly.
221.	Financial Intermediaries Association of Southern Africa (FIA)	8.6.6 – Remediation Management	We request that a proportional approach be applied here. For smaller Category II FSPs, these requirements are particularly onerous.	This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect, detect, respond and recover from cyber incidents. A cyber incidents may have a disastrous impact on the financial institution and financial customers. Also see response to comment 201 above.
222.	Standard Bank Group	8.6.6 Remediation management (b)	Major issues may only be found post deployment (eg Log4J). Suggest change to: **Known** major issues and software defects must be remediated before production deployment; and	Noted. The Joint Standard has been updated accordingly.
223.	Investec	8.6.6b	Suggest removing reference to "software defects" as this is beyond the scope of a security standard; the requirement should refer to "security flaws" or similar terminology.	Noted, 'software defects' have been changed to 'security flaws'.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
224.	Purple Group Limited ("Purple Group")	8.7.1(a)	Please provide guidance on what this requirement entails from a practical perspective. How would a financial institution implement this? For example, is it sufficient to update a financial institution's cybersecurity software regularly to comply with this requirement?	People, process and systems must evolve and adapt.
225.	Investec	8.7.1a	Propose splitting into two requirements. Have a separate point for "systematically identify and distil key lessons from cyber events that have occurred within and outside the institution in order to advance resilience capabilities".	Cyber resilience capability includes people, process and technology. The definition of cyber resilience has been amended to include 'People, process and technology.
226.	Two Mountains	8 2.3 a iv	"Strong access control mechanisms" define a baseline / standard or reference a framework	See response to comment 120 above.
227.	Two Mountains	8.2.1	How do we define "as appropriate and effective"? What is the baseline and framework that is referred to here as appropriate or effective?	Effective and appropriate must be assessed in consideration of the nature, scale and complexity and risk profile of the financial institution. See response to comment 15 above.
228.	Two Mountains	8.2.3 a ii	Again, referenced to appropriate – need some baseline on what is deemed appropriate. Suggest adding appropriate and also effective as part of the definitions in Point 4	See response to comment 226 above.
229.	Two Mountains	8.2.3 a vii	"Adequate processes" what is defined and deemed as	See response to comment 226 above

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			adequate? Suggest adding Adequate processes to the Definitions list in Point 4	
230.	Two Mountains	8.2.3 a viii	"Appropriate controls" what is defined and deemed as appropriate? Suggest adding Appropriate controls to the Definitions list in Point 4	See response to comment 226 above.
231.	Two Mountains	8.6.1 a	Spelling mistake "teffectiveness"	Noted and amended.
232.	Two Mountains	8.6.1 c ii	Timely Manner – How many days is a timely manner? Timely Manner means a period of **thirty days**, unless this period is shortened by the existence of an emergency.?	See response to comment 196 above.
233.	Two Mountains	8.6.2 a i	Timely Manner?	See response to comment 198 above.
234.	Two Mountains	8.6.4 a i	Regular – what is deemed as regular? Quarterly / annually?	See response to comment 216 above.
235.	Two Mountains	8.6.5 a ii	May the institution select its own standards on secure coding? No reference made to a defined or framework to be measured against	Yes, provided that it is appropriate considering the nature, scale, complexity and risk profile of the financial institution.
236.	Two Mountains	8.6.6 c	Timely Manner – recommended to define Timely manner under Point 4 Definitions and interpretations. Constant reference to a time that is not defined.	It depends on the institution and the nature of the vulnerabilities.
237.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and	9. Cybersecurity hygiene practices (9)	No comment.	Noted.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
	OUTsurance Life Insurance Company Limited			
238.	Aurora Insurance Company	9.1 – 9.7	Duly Noted.	Noted.
239.	First rand Group	9.1.1 (c)	"apply the principles of 'segregation of duties', and 'least privilege' when granting user access to information assets **so that no one person has access to perform sensitive IT system functions.** Access rights and privileges must be granted according to the roles and responsibilities of the user;" Highlighted wording needs clarification as it is ambiguous – does it mean nobody must be given access to perform sensitive IT system functions or does it mean that there shouldn't be key man dependency here?	Noted. The paragraph has been amended as follows: (c) apply the principles of 'segregation of duties', and 'least privilege' when granting user access to information assets. ~~so that no one person has access to perform sensitive IT system functions~~. Access rights and privileges must be granted according to the roles and responsibilities of the user;
240.	Allan Gray	9.1.1 paragraph (c) This segregation may be harder for smaller FSP's	9.1.1 paragraph (c) This segregation may be harder for smaller FSP's	This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect, detect, respond and recover from cyber incidents. A cyber incidents may have a disastrous impact on the financial institution and financial customers.
241.	Investec	9.1.1a	Need to consider what this means if an institution goes	Noted. The paragraph has been amended as follows:

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			passwordless for authentication (e.g., Windows Hello).	(a) establish a security access control policy (which includes identity and access management such as passwords, biometrics, tokens etc), and a process to enforce strong security controls for users' access to IT systems;
242.	First rand Group	9.2.1 (c)	Suggest the paragraph: "establish a process to manage and monitor the use of IT systems and service accounts for suspicious or unauthorised activities." Be reworded as: "establish a process to manage and monitor the use of **critical** IT systems and service accounts for suspicious or unauthorised activities." Such as to maintain practicality and affordability of resources	This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect, detect, respond and recovery from cyber incidents. The impact of a cyber incidents has disastrous impact on the financial institution and financial customers.
243.	Standard Bank Group	9.2.1 Privileged access management A financial institutions must – (a)	ensure that every administrative account in respect of any **cloud tenant, authentication system,** operating system, database, application, security appliance or network device, is secured to prevent any unauthorised access to or use of such account;	Noted. The paragraph has been amended as follows: ensure that every administrative account in respect of any operating system, database, application, security appliance; network device, cloud tenant or, authentication system is secured to prevent any unauthorised access to or use of such account;
244.	BrightRock	9.3	Multi-factor authentication. There has been different	Multifactor authentication is two or more factors.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			definition to multifactor authentication. The book definition being authentication using three forms which could be something a user have, something a user is and something a user know. Lately in the business industry many forums refer to two-factor authentication as multifactor authentication. Can this topic be specified to avoid confusion?	
245.	First rand Group	9.3.1 (b)	Consider rephrasing to: "ensure that MFA is implemented for all administrative accounts related to any operating system, database, application, security appliance or network device **deemed critical to the institution's cyber resilience**"	This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect, detect, respond and recover from cyber incidents. A cyber incidents may have a disastrous impact on the financial institution and financial customers.
246.	CitiBank NA South Africa	9.3.1 (b) which requires us to implement Multi-Factor Authentication (MFA) for all administrative accounts at Operating System, database, security appliances and network devices	Citi has adopted a risk-based approach to the implementation of multi-factor authentication where this is required. We enforce it for: a) all our internet facing platforms if there are logins required. b) All applications handling high value transactions (threshold currently linked to a monetary value) c) All remote access connections	The MFA in 9.3.1(b) is only related to administrative accounts and not for all operating systems etc. See requirements for MFA for systems in 9.3.1(a) - which relates to only critical system functions. The paragraph has been amended to avoid confusion as follows: (b) ensure that MFA is implemented for all administrative and privileged accounts ~~related to any operating system, database, application, security appliance or network device;~~ and

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			d) Any other connection which is deemed high risk by the business. Requiring it for all administrative, operating systems, security appliances and network devices will create a major security challenge due to either lack of ability to deploy this control or very costly to add third party tools to provide the authentication.	
247.	China Construction Bank Corporation Johannesburg Branch	9.3.1 Multi factor authentication – B	States MFA is implemented for all administrative accounts for O/S, database, network devices etc – does this relate to all infrastructure servers and network devices or only those that house critical or transactional information systems? For example a server set up as a print server vs a SQL server.	Disagree – MFA must apply to all administrative accounts irrespective of criticality of the system.
248.	Standard Bank Group	9.3.1 Multi-factor authentication (MFA) A financial institutions must – (b)	ensure that MFA is implemented for all **privileged accounts**	Noted. The paragraph has been amended to include privileged accounts. (b) ensure that MFA is implemented for all administrative and privileged accounts ~~related to any operating system, database, application, security appliance or network device;~~ and
249.	ASISA	9.3.1(b)	The use of MFA is a good control and are supported. However, the term “application” causes confusion, and it is not clear how	Noted. The paragraph has been amended to remove confusion as follows: (b) ensure that MFA is implemented for all administrative and privileged accounts ~~related to any~~

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			the requirements in this paragraph differ from what is covered in Paragraph 9.3.1(a). It is suggested that Paragraph 9.3.1(b) be removed: --- ~~"ensure that MFA is implemented for all administrative accounts related to any operating system, database, application, security appliance or network device"~~	~~operating system, database, application, security appliance or network device;~~ and
250.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	9.3.1(b) & 9.7.1	• Assuming 3rd party providers are required to comply with the standard; there are cost implications on the 3rd Party providers which may not be recoverable. • Paragraph 9.3.1 (b) Please could the Authorities clarify which types of "applications" fall within the scope of this requirement? Kindly clarify what an "administrative account related to any application" may be. Are administrative accounts on critical systems included in this requirement?	This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect, detect, respond and recovery from cyber incidents. A cyber incidents may have a disastrous impact on the financial institution and financial customers. Third party Security providers must implement the same or equivalent security controls as the financial institution. Noted. The paragraph has been amended to remove confusion as follows: (a) ensure that MFA is implemented for all administrative and privileged accounts ~~related to any operating system, database, application, security appliance or network device;~~ and Noted. The paragraph has been amended as follows: (a) implement endpoint protection, ~~which includes but is not limited to behavioural-based and signature-based solutions,~~ to protect a financial institution from malware infection and address

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			Paragraph 9.7.1 We propose that the focus on the section should be more on the expected outcomes rather than on the type of tools used (behavioural or signature based).	common delivery channels of malware, such as malicious links, websites, email attachments or infected removable storage media;
251.	ASISA	9.3.1(c)	It is assumed that "user accounts" does not refer to client accounts, as there are other measures in place for clients when accessing their own sensitive information. For intermediaries, that access multiple clients' information, there is no MFA in place at this stage. If required, it would have a material impact and as such the Regulator must indicate if that is expected.	User account does not include customer accounts, however your intermediaries are not clients but rather users and there must use MFA to access client accounts.
252.	Investec	9.3.1b – c	The requirement is a little ambiguous. It is not clear if this refers to access to resources via the internet (e.g., cloud portals), or to remote access to internal systems. The intention seems to be that MFA is used to access applications with sensitive information via the Internet. The current wording can be misunderstood to relate to browsing. Thus, suggest proposed wording: "ensure that MFA is implemented for all user accounts utilised to access	Noted. The paragraph has been amended to include privileged accounts. (b) ensure that MFA is implemented for all administrative and privileged accounts ~~related to any operating system, database, application, security appliance or network device~~; and In addition, paragraph (c) ensure that MFA is implemented for all user accounts utilised to **access applications containing sensitive information** through the internet. The Joint Standard is requiring MFA as a minimum requirement.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			applications containing sensitive information via the internet". And even so this may not be practical and other controls could be sufficient, such as security certificates on the device with conditional access policies.	
253.	Standard Bank Group	9.4 Network perimeter defence	Suggested addition: Ensure that the network is protected from disruption (eg Denial of Service attacks)	Noted. The paragraph has been amended to include 'disruption'. Added as paragraph (a) ensure that the network is protected from unauthorised access and disruption
254.	BASA	9.5.1 (a)	**Recommend** rephrasing to: " address vulnerabilities to critical IT systems, by applying such security patches or other mitigating controls as possible, within a timeframe that is commensurate with the risks posed by each vulnerability; Patching is frequently not possible on a timely basis due to the interplay between applications, databases, operating systems and including time to assess.	Agree, and amended as follows: it addresses vulnerabilities to critical IT systems, by applying security patches or other mitigating controls as possible, within a timeframe that is commensurate with the risks posed by each vulnerability
255.	First rand Group	9.5.1 (a)	Suggest rephrasing to: " address vulnerabilities to critical IT systems, by applying such security patches or other mitigating controls as possible, within a timeframe that is	See response to comment 254 above.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			commensurate with the risks posed by each vulnerability; This is because patching frequently not possible on a timely basis due to interplay between application, DB and OS, including time to test in some circumstances.	
256.	Silica Administration Services (Pty) ltd	9.5.1(c)	To add: "where possible"	Disagree, all patches must be tested before being implemented into the production environment.
257.	BASA	9.6	Some banks do not keep security standards separate for the general implementation standard of a specific device, operating system, etc. This is based on the mindset of always security by design and as such, security is built into the design and not an add-on. **Recommend** that this be taken into consideration when collecting evidence to support compliance to these standards,	Noted.
258.	BASA	9.6 (a)	**Recommend** limiting and simplifying the requirement. There is too much detail here for a standard and the variance between all of those details is confusing.	Noted. (a) ensure that there is a written set of security standards for hardware and software, ~~including but not limited to, operating systems, databases, network devices and endpoint devices~~. New (b) Ensure that the security standards must outline the configurations that will minimise the financial institution's exposure to cyber threats;
259.	Investec	9.6.1a	Clarify that security standards must be defined, and may be	The paragraph has been amended to delete the types of devices.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			included in standards for hardware, software, OS's, databases, etc. – this requirement should not mandate a security standard document for each type of tech as this is not practical or necessary to be separated from the overall standard of the tech. Suggest a statement that "security requirements must be included in technology standards".	
260.	Investec	9.7.1c	Suggest changing "scanning of indicators" to "scanning for indicators of compromise"	It has been amended – change 'of' to 'for'
261.	Rand Mutual Assurance	Exemption from 8.2.3(a)(ix) – Permanent deletion of sensitive data	Under POPIA application for exemption to this requirement can be applied for to the Information Regulator – however it seems that this section is in contradiction to POPIA.	Exemptions also apply to the Act and the Joint Standard. This paragraph has been amended – see response to comment 129 above.
262.	Bank Zero Mutual Bank	None	None	Noted
263.	Bank of China	None	None	Noted
264.	Assent	None	None	Noted
265.	Masthead	7.1.2 Section 7 - Cybersecurity strategy and framework	s7.1.2 Since the cybersecurity strategy of a financial institution must be reviewed at least annually, we do not see the need to include the word "regularly". A change along these lines would also, in our view, align to the timeframe required in s7.1.6.	Regularly relates to where there is a need to change the strategy because of some incident etc.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
266.	Masthead	7.2.2 Section 7 - Cybersecurity strategy and framework	s7.2.2 Our comment above (in relation to s7.1.2) applies equally here – we see no need to include the word “regularly” in light of the requirement that the cybersecurity framework must be reviewed at least annually. The implementation of a requirement for 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. This Joint Standard (s 3.5) already requires 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 apply their rationale in deciding whether the nature of the business requires an external and independent party to review and update its policies, standards and procedures. We would therefore suggest that there is no need for the words “…through independent compliance programmes and	See comment 265 above. Independent review can be done internally, and financial institutions do not need to appoint an external party.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			audits carried out by qualified individuals…" in s7.2.2 and that they be deleted. This would further, in our view, support the regulator's move to more principle-based regulation.	
267.	Masthead	Section 8 - Cybersecurity and cyber-resilience fundamentals	General comment/observation Viewed from a compliance and business perspective, we find the requirements set out in this section detailed and prescriptive. We wonder to what extent this is aligned to the objective set out in s3.5 and therefore whether there is the right balance between principles and rules.	This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect, detect, respond and recover from cyber incidents. A cyber incident may have a disastrous impact on the financial institution and financial customers.
268.	Masthead	Section 8 - Cybersecurity and cyber-resilience fundamentals – Identification	s8.1.3 Similar to our comments above (in relation to s7.1.2 and 7.2.2), we see no need to include the word "regularly".	As these list change frequently, it is important to review it regularly.
269.	Masthead	Section 8 - Cybersecurity and cyber-resilience fundamentals	s8.6; s8.7 The implementation of a requirement of mandatory testing and learning and evolving comes with an added and potentially high cost impact for FSPs as these specialist services will likely be outsourced to third-party providers. This Joint Standard already requires	This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect, detect, respond and recover from cyber incidents. A cyber incident may have a disastrous impact on the financial institution and financial customers

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			that financial institutions should apply a proportionate and risk-based approach which is suitable to their organisation size and nature. Therefore, in our view, it should be left to the financial institution to apply their rationale, based on the nature of the business, to decide on the type of testing and the nature of learning and evolving that is required in terms of its policies, standards and procedures.	
270.	Masthead	Section 8 - Security Hygiene Practices	Similar to our comment above, the implementation of mandatory security hygiene practices such as Multi Factor Authentication (MFA) and Malware requirements that are listed in Section 8, comes with an added and potentially high cost impact for FSPs. This Joint Standard already requires that financial institutions should apply a proportionate and risk-based approach which is suitable to their organisation size and nature. Therefore, in our view, it should be left to the financial institution to decide, based on the nature of the business, what type of security hygiene practises are required.	This Joint Standard contains minimum requirements for cybersecurity and cyber resilience. This enables financial institutions that deal with public funds to be able to identify, protect, detect, respond and recover from cyber incidents. A cyber incident may have a disastrous impact on the financial institution and financial customers.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
271.	Financial Intermediaries Association of Southern Africa (FIA)	10 – Regulatory Reporting	Clarity is requested on what is meant by 'any' cyber incident.	Noted. The paragraph has been amended.
272.	Rand Mutual Assurance	10 – Regulatory Reporting	10.1 requires FI's to report to the Authorities of any system failure, malfunction, delay, or incident within 24 hours if no obligation exists under another financial sector law. All the items covered in these standards can be linked to a section of POPIA and the authority of the Information Regulator. Will there be a dual reporting requirement on FI's, or can it be assumed that such incidents will always be reported to the IR?	As these are being dealt with by different regulators with different mandates, dual reporting is required where necessary.
273.	Standard Bank Group	10. Regulatory reporting	The proposed Joint Standard stipulates that the Authorities need to be notified of the following: **'material systems failure, malfunction, delay or other disruptive event, or any cyber incident, within 24 hours of classifying the event as material'.** The request is for the Authorities to provide guidance on the parameters of what is deemed 'material' in the context of the proposed Joint Standard.	The institution is responsible for classifying material system failure and malfunctions.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
274.	Hollard	10. Regulatory reporting	i. Where reporting needs to be submitted to needs to be specified in the proposed Joint Standard. With joint standards as well as the Information Regulator requirements, it is expected that there will be lots of unintentional overlap with regards to reporting obligations. There needs to be greater co-operation between the various regulators (including the FSCA and PA) to make sure multiple reports are not required multiple times and there is one repository that the reports can be sent to. The reporting template needs to be defined and attached as an addendum to the proposed Joint Standard for comment.	When the Joint Standard goes out for formal consultation – the reporting template will be submitted for consultation.
275.	Hollard	10. Regulatory reporting/ 10.1	i. Clause 10.1 requires a definition of material. Material is subjective. ii. The paragraph should read that notification is required within 24 hours, not reporting. Reporting will require investigation that will take longer than 24 hours. Where a cyber event or cyber incident is only	As these are being dealt with by different regulators with different mandates, dual reporting is required where necessary. The institution is responsible for classifying material system failure and malfunctions. The reporting template provides details of how and what to report.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			discovered later, the 24-hour requirement cannot apply. " …within 24 hours of classifying the event as material" should read "within 24 hours of discovering and classifying a cyber incident as material." We should not be reporting on cyber events. Only material (to be defined) cyber incidents should be reported.	
276.	Hollard	10. Regulatory reporting/ 10.2	The time, manner and period for regulatory reporting must be defined in the proposed Joint Standard for comment.	The form of reporting as well as the timing will be communicated in the reporting template which will be published for comment during the formal consultation process.
277.	BASA	10.1	**Recommend** adding the word 'material" to the highlighted wording so it reads as follows: "**or any material cyber incident."**	Cyber incidents classified as material must be reported. Material is added at the end of the sentence.
278.	Bidvest Bank	10.1	This is a duplication of the requirements as set out in Directive 2 of 2019 and it is recommended that it be removed.	Directive 2 will be repealed when the Joint Standard is finalised.
279.	Silica Administration Services (Pty) ltd	10.1	24hours is not practical. Rather consider "as soon as reasonably possible".	24 hours is only after classifying the event as material. The reporting template will provide more detail on the information required. Please note that this paragraph has been amended in respect to the 24 hours.
280.	First rand Group	10.1	This reporting requirement seems like a duplication of Directive 2 of 2019 "Reporting of	Directive 2 will be repealed when the Joint Standard is finalised.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			material IT and/or cyber incidents". Suggest removing this if there wont be any other reporting requirement relating to this Cyber standard.	
281.	First rand Group	10.1	For clarity, suggest adding the word 'material" to the highlighted wording so it reads as follows: "**or any material cyber incident".**	Cyber incidents rclassified as material must be reported. Material is added at the end of the sentence.
282.	ASISA	10.1	For financial institutions that are supervised by both Authorities, it is suggested that the requirement to notify the Authorities is streamlined to form part of a joint process which caters for the reporting obligation as per this paragraph. Financial institutions that are only being supervised by one financial sector regulator, should only be required to inform the responsible Authority of any material systems failure, malfunction, delay or other disruptive event, or any cyber incident. It is suggested that paragraph 10.1should be amended as follows: ---------- "A financial institution must, unless such a reporting obligation already exists in another financial sector law,	The paragraph has been amended to require reporting to the responsible authority.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			notify the **responsible** Authoriti~~es~~**y**, in the form and manner determined by the Authorities, of any material systems failure, malfunction, delay or other disruptive event, or any cyber incident, within 24 hours of classifying the event as material."	
283.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	10.1	It is our recommendation that point 10.1 of the Standard needs to be more specific and clearly defined so that is clear who will determine the materiality i.e. will it be the financial institution or the Regulator.	The financial institution must classify materiality.
284.	ENSAfrica	**10.1** 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 cyber incident, within 24 hours of classifying the event as material. As read with the definition of "Authorities" under section 1	Reference to "Authorities" as read with the definition thereof under section 1 suggests that the financial institution must notify both the Prudential Authority and Financial Sector Conduct Authority. It may be impractical for certain financial institutes to notify the Prudential Authority, and others the Financial Sector Conduct Authority. We propose that reference to the first "Authorities" be amended such that it reads "the Authority responsible for the financial institution" (see for example the way in which this term is used in	The paragraph has been amended to refer to the responsible authority.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			the FSRA, section 5 read with schedule 2). Similarly we propose that the definition of "Authorities" be amended to include "and Authority shall mean any one of them as the context may require".	
285.	ENSAfrica	**10.1** 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 cyber incident, within 24 hours of classifying the event as material.	In the first instance, we are of the view that this reporting obligation may give rise to a number of interpretational difficulties, being as follows: • we are left to assume that "such a reporting obligation" refers to an obligation in another financial sector law dealing with "material systems failure, malfunction, delay or other disruptive event, or any cyber incident". The difficulty with this, as is further outlined below, is that the words "material systems failure, malfunction, delay or other disruptive event" are quite opaque and therefore open to interpretation and other financial sector laws may not use similar	Directive 2 of 2019 relating to banks will be repealed once the Joint Standard is finalised. Due to the fact that this Joint Standard applies to various financial institutions with different natures, scales, complexities and risk profiles it falls within the duty of financial institutions to determine what is a material failure, malfunction etc. The Authorities have however, defined material incident to assist financial institutions with their categorisation. The paragraph has been amended to allow the Authorities to determine the time period (previously 24 hours) within which a financial institution must report to the Authorities after classifying an event as material. The Authorities will monitor this from a supervisory perspective and make any necessary amendments to the reporting template and issue guidance if necessary. We have amended the Joint Standard to make the requirements clearer as follows: A financial institution must notify the responsible authority for the financial sector law under which the financial institution is registered or licensed, after classifying the following as material incident: • cyber incident; or

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			wording to categorise the same event. As such, it is more likely that financial institutions will err on the side of caution and report to the authorities under the Draft Joint Standard and also report to the relevant authority (who will in most instances be the Authorities) under a financial sector law in any event. This will result in multiple notifications to the same authority; • an assessment of each of the financial sector laws must be made in each instance or an incident to determine whether the issue is notifiable in terms of some other law. Again, it is more than likely that financial institutions will err on the side of caution and duplicate their reports. In addition, to undertake this assessment on each occasion of a notifiable event, may add significant	• information security compromise. The reporting in terms of paragraph 10.1 above must be made in the form and manner as well as within the timeframes determined by the Authorities. The Authorities will monitor this from a supervisory perspective and make any necessary amendments to the notification /reporting template and issue guidance if necessary. The interpretation was correct, the financial institution must only report 24 hours after classifying the event as material. Please note that the 24 hours removed has been removed from the Joint Standard and will captured in the notification template.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			complexity when the financial institution is under pressure and should be focusing efforts on mitigating the events of the incident; and • it is not clear whether "all" cyber incidents must be reported or whether only a "material" cyber incident would need to be reported. If the first part of the sentence is considered, then it would appear that the reporting obligation applies to any cyber incident, with no materiality threshold. However, the second part of the sentence which relates to the timing of the report, provides that a report must be made "within 24 hours of classifying the event as material". This means that an event must only be reported within 24 (twenty four) hours of classifying the event as "material", not that the event must be	

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			reported within 24 (twenty four) hours of the financial institution becoming aware of the event in question. Some may even go so far as to ask whether a cyber incident would fall within the meaning of an "event" which is used in the latter part of the sentence. In the second instance, and regarding the threshold to report, if a report must only be made after classifying the event as material, what would the consequences be if a financial institution did not classify the event in question as material and therefore did not report to the Authorities. Would the Authorities later question the financial institution's characterisation of the event as non-material and what would the consequence of an incorrect classification be? Again, financial institutions are likely to err on the side of caution and resort to reporting all incidents regardless of materiality. In the third instance, if it was rather intended that a financial institution should report an	

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			incident within 24 hours of discovering it (which in our view is not the current requirement on a reading of this section), then this may not be sufficient time for a financial institution to assess the incident in question and properly report on same. In this regard, it would be helpful to obtain some clarity from the Authorities regarding: • the threshold to report; • the point at which the clock starts to run in order to make a notification; and the form and level of detail which will be required in the initial report.	
286.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	10.1	• Paragraph 10.1 makes reference to classification of an "event as material" without defining material, it is therefore proposed that material be defined in order to avoid confusion. Further, the paragraph makes reference to 24-hour reporting period. Furthermore, we propose the word	Due to the fact that this Joint Standard applies to various financial institutions with different natures, scales, complexities and risk profiles it falls within the duty of financial institutions to determine what is a material. The paragraph has been amended to allow the Authorities to determine the time period (previously 24 hours) within which a financial institution must notify the Authorities after classifying an event as material. A definition of material incident has been inserted. Noted, the heading has been changed to notification and reporting requirements. Because financial institutions deal with public funds 24 hours after determining that the event was material is considered sufficient by the Authorities.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			"reporting" be replaced with "notifying" We propose that the reporting be aligned with Cybercrime Act 19/2020 in terms of reporting time which is 72 hours. Furthermore, the 72 hours will enable the financial institution adequate time to comprehensively investigate the incident and provide the required information. • We request the Authorities to streamline the reporting process to caters for one reporting as opposed to dual i.e.to the FSCA & PA.	However, the time period has been removed from the Standard and will be included in the notification template that will be determined by the Authorities. The Joint Standard has been amended accordingly.
287.	Aurora Insurance Company	10.1 – 10.2	Duly Noted.	Noted.
288.	Two Mountains	10.1	"Determined by Authorities" How is this determined? Randomly or is there a set way? What systems, are we referring to the core systems to run the insurance business or any system in the organisation?	A determination is a formal instrument that the Authorities will use to implement the reporting/notification requirements. The notification requirements will be published with the Joint Standard in the next consultation process.
289.	First rand Group	10.2	"The Authorities, may in addition to the requirements of paragraph 10.1 above,	The notification template will be published for comment when the Joint Standard is published for formal consultation.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			determine the time, manner and period for regulatory reporting for this Joint Standard.”. This does not enable the member organisations to gauge the extent of compliance and reporting demands that will be imposed by this standard, as well as the likely impact (financial, operational) to existing Assurance providers. If possible, try and articulate those requirements upfront.	
290.	ENSAfrica	**10.2** The Authorities, may in addition to the requirements of paragraph 10.1 above, determine the time, manner and period for regulatory reporting for this Joint Standard	This provision implies that financial institutions may, in future, be required to report on their compliance (including manner of compliance) with the Joint Standard. Should this indeed be the intention behind this provision, then the Authorities should be alerted to the security risks inherent in financial institutions disclosing their approach to cybersecurity in granular detail to third parties, even if that third party is the PA or FSCA. This information in the hands of malicious actors would provide a blueprint for circumventing a financial institutions cybersecurity safeguards.	This concern is noted. However, the Authorities are empowered to view vulnerability assessments, penetration testing results etc. during supervisory interventions.
291.	OUTsurance Holdings Limited,	11. Short title	No comment	Noted.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
	OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited			
292.	Aurora Insurance Company	11.1	Duly Noted.	Noted
293.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	Short title	No Comment	Noted
294.	Willis Towers Watson	General comments	(Our comments are mainly in Section C. We have no objection if the Authorities wish to publish these comments, including those in Section C.)	Noted.
295.	Nedbank Limited	General comments	Participated in the BASA process	Noted.
296.	Equity Express Securities Exchange (Pty) Ltd	General comments	None	Noted
297.	The Federated Employers Mutual Assurance Company (RF) (Pty) Ltd	General comments	None	Noted.
298.	The Cape Town Stock Exchange	General comments	None	Noted.
299.	Integrity Retirement Fund Administrators (PTY) Ltd		None	Noted.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
300.	Habib Overseas Bank Limited	0.All sections	Agree with the proposed wording	Noted.
301.	Clientele Limited	0.None	None	Noted.
302.	Rand Mutual Assurance	Exemptions	There is no process listed to FI's to apply for exemption from any of the set standards.	The process for exemptions is catered for in terms of section 281 of the Financial Sector Regulation Act.
303.	Rand Mutual Assurance	Authority of Information Regulator	Please provide clarity as to whether the IR's authority will take precedence over the FSCA / PA in the event of an investigation / incident or breach?	The regulators have different mandates. The financial institution must comply with the requirements imposed by the different regulators.
304.	Rand Mutual Assurance	Penalties	There is no clarify on the penalties for FI's in the event of breach / non-compliance to any of the standards. Example: what sanctions will a FI face if its staff is not trained at least annually on Cybersecurity awareness?	These are dealt with in terms of the FSR Act and the regulatory action policies of the Authorities.
305.	Rand Mutual Assurance	POPIA overlap	There is no mention of POPIA in the Standards (only the FSR Act). Is there a reason for excluding POPIA from the Legislative authority in paragraph 2?	A financial institution must comply with all applicable legislation. It is not necessary to list all the related legislation.
306.	Two Mountains	Annexure 11.1	What standard is this aligning with? There is international best practice as set out by ISO 27001, CIS, PoPIA etc.	The Authorities have considered a number of international standards/best practices (including CPMI/IOSCO) in drafting the minimum requirements and principles contained this Joint Standard.
307.	Institute of Retirement Funds Africa	3.9	Paragraphs 3.9, 3.10, 3.11 and 6.7 read consecutively raise a serious concern. The law as	The proposed Joint Standard outline the minimum requirements and standards to be implemented by the regulated entities. The Joint Standard aims to

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			prescribed will be interpreted according to the subjective challenges faced by the different financial institutions and as such the implementation of anti-cyber attacks will leave loopholes. For example, a scenario whereby a institution (A) invests hefty amounts into their online programme to protect their retirement platform and a fairly new investment institution (B) does not creates loopholes, for example by way of section 14 transfers. A heavily invested anti cyber-attack company will have the means to guard against any attack. However, if another company (B) is comprised then hackers can use B to access A's platform and their clients' information respectively. As a result, a codified anti-cybercrime attack system might resolve this problem and assist companies to function at a vigilant level regardless of financial backing. Therefore, the submission is that the scope of this Standard should be extended to IT professionals to share ideas on these challenges. In closing, following the same legislation is not enough to curb these challenges. Sharing of a more	strengthen the management of the cybersecurity risk in a manner that will ensure consistency across the different regulated entities, which would enhance the protection of financial customers and improve the overall resilience of the financial services ecosystem. The Joint Standard will be implemented and assessed in consideration of the nature, size, complexity and risk profile of a financial institution. The Joint Standard only applies to the supervised entities and places obligations on the entities. There is definitely the role of IT professionals in the implementation of the Joint Standard to ensure compliance. However, the Authorities do not agree with the proposal for the scope of the Joint Standard to be extended to IT Professionals.

Table 6 – Full set of comments received during the consultation held in 2021

No.	Commentator	Paragraph	Comment	Response
			practical day to day regime is required.	