FSCA
Financial Sector Conduct Authority

South African Reserve Bank
Prudential Authority

Comments received on the Draft Joint Standard on Cybersecurity and Cyber Resilience Requirements for financial institutions as at the close of the commenting period on 28 February 2022

September 2022

Contents

List of Commentators

No	Name of organisation	Contact Person and Contact Details
1.	Clientèle Limited (including Clientèle Life Assurance Company Limited and Clientèle General Insurance Limited)	Malenthren Govender
2.	Habib Overseas Bank Limited	Rehan Zaidi / Neo Motlagomang
3.	Standard Bank Group	Robin Barnwell
4.	Masthead	Anri Dippenaar
5.	Bank Zero Mutual Bank	Jayesh G Prag
6.	Bank of China	Rookeya Salajee
7.	Willis Towers Watson	Dr Erich Potgieter (Associate)
8.	BASA	Benjamin April
9.	Deutsche Bank AG	Johan Gibhard
10.	Assent	Freddie Eilers
11.	Alan Gray	Werner Lunow
12.	ASISA Association for Savings and Investment - South Africa Consolidated submission on behalf of ASISA Members	Johann van Tonder
13.	Silica Administration Services (Pty) ltd	Eugene Venter
14.	FirstRand Group	Kovelin Naidoo
15.	Nedbank Limited	Lianca du Toit
16.	Financial Intermediaries Association of Southern Africa (FIA)	Samantha Williams
17.	BrightRock	Lyton Simbanegavi
18.	Bidvest Bank	Jaco De Beer
19.	Equity Express Securities Exchange (Pty) Ltd	Nikki Clackworthy
20.	Johannesburg Stock Exchange	Anne Clayton
21.	The Federated Employers Mutual Assurance Company (RF) (Pty) Ltd	Gys Mc Intosh
22.	Purple Group Limited (“Purple Group”)	Sascha Graham
23.	A2X Markets	Luthfia Akbar/ Gary Clarke
24.	SA Home Loans	Mark Dand

25.	MTN SA	Isack Ngobeni
26.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	Maretha Hurter
27.	China Construction Bank Corporation Johannesburg Branch	Shannon Delpeche
28.	Investec	Carmel Lerner
29.	Aurora Insurance Company	Angie Botha
30.	ENSAfrica	Rakhee Dullabh, Jessica Blumenthal
31.	Just Retirement Life (South Africa)	Thiren Pillay
32.	The Cape Town Stock Exchange	Hannes van der Merwe
33.	Integrity Retirement Fund Administrators (PTY) Ltd	Fritz Wasserfall
34.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	Ntsoaki Ngwenya
35.	Hollard	Ntokozo Magasela
36.	AIG	Fiona Oakley-Smith
37.	Institute of Retirement Funds Africa	Wayne Hiller van Rensburg
38.	Rand Mutual Assurance	Juanita Moolman & Ben Lourens
39.	Two Mountains	Lindani Ngema
40.	Citibank Na South Africa	Edward Kiptoo

Comments received

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
1. Commencement				
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 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.	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.
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 another revision of the Joint Standard before commencement?	See response to comments 2 and 3 above. The revision depends on comments raised.
2. Legislative authority				
5.	The South African Insurance Association (SAIA), a representative body of the non-	2	No comment	Noted.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
	life insurance industry			
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.
3. Application				
9.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	3	No comment	Noted.
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

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
				order to eliminate any confusion, the word 'potential' in relation to risks has been deleted.
14. 1	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.
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 <u>all</u> 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 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 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.	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.
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	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			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 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?	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.
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 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.	The exemption process is covered in section 281 of the FSR Act.
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 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.	Refer to the response to comments 15 and 16 above.
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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
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 the recommendation of MTN SA that this be highlighted in the proposed Joint Standard.	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 impractical to specify all the applicable legislation that have common areas of application.
4. Definitions and interpretation				
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.
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 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.	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
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 clarity and consistency, we recommend that either of the terms 'sensitive information' or 'sensitive data' is used throughout the Joint Standard.	. 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.
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 cyberattack". "Observable occurrence" could for example be running out of disk space, which should not qualify as a cyber event.	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.
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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
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. • 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.	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'. 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.
5 – Roles and responsibility				
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 avoidance of uncertainty, it is the recommendation of MTN SA that the definition of "governing body" be clearly defined.	Noted. The definition of a governing body is provided in the Financial Sector Regulation Act, 2017.
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. 18	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	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 be very different for a smaller organisation.	See response to comment 44 above.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
	Southern Africa (FIA)			
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 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.	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.
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 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	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.
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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
6. Governance				
57.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	6	No comment	Noted.
58.	Hollard	6.1	Duly Noted.	Noted.
59.	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.
60.	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.
61.	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 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 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.	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 digitalmedium. 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, 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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
62.	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.
63.	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 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.	Noted, the paragraphs have been amended accordingly.
64.	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 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).	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.
65.	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 resolution thereof. Clarity on the expectation is important.	See response to comment 61 above.
66.	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.
67.	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."	See response to comment 61 above.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			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 structured in line with regulatory expectations.	
68.	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
69.	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: -------- " 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.**"**	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'.
70.	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.
71.	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.
72.	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.
73.	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	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

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			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 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…	
74.	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.
7.Cybersecurity strategy and framework				
75.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	7	No comment	Noted.
76.	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 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 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	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			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.	
77.	Aurora Insurance Company	7.1 – 7.2	Duly Noted.	Noted.
78. 31	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.
79.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	7.1.5	• Paragraph 7.1.5 makes reference to "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.	The Authorities will not prescribe the industry standard. However, through supervision, the Authorities will assess based on the nature, scale, complexity and risk profile whether the industry best practice that is implemented by the financial institution is adequate.
80.	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.
81.	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.
82.	Investec	7.1.6	Unclear on what is required in the statement "annually define and quantify business risk tolerance relative to cybersecurity" and if a separate standalone statement is expected, in addition to cyber related risk tolerances defined through operational risk management.	Noted. The paragraph has been amended to read: "Define and reassess regularly business risk tolerance relative to cybersecurity and ensure that it's consistent with the business strategy and risk appetite; and .
83.	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'.
84.	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.
85.	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: --- "Be reviewed regularly, but at least annually**, by an internal control function** for adequacy and effectiveness through independent compliance programmes ~~and audits carried out by qualified individuals~~; and"	Noted. See response to comment 84 above.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
86.	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.
8.Cybersecurity and cyber-resilience fundamentals				
87.	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.
88.	Hollard	Cybersecurity and cyber-resilience fundamentals/ 8.1.2 (a)	Spelling error: “providerss”	Noted and amended.
89.	Hollard	8. Cybersecurity and cyber-resilience fundamentals/ 8.2.1	Add “or cyber incident” to the end of the paragraph.	Noted, added cyber incident.
90.	Hollard	8. Cybersecurity and cyber-resilience fundamentals/ 8.6.1 (a)	Spelling error: “teffectiveness”	Noted. See revised Joint standard.
91.	Aurora Insurance Company	8.1 – 8.7	Duly Noted.	Noted.
92.	BASA	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. **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.	Noted. Paragraph 8.1.1 has been removed as it has been incorporated in 8.1.2 (b) and (c)
93.	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.
94.	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.
95.	First rand Group	8.1.2 (a)	Spelling error - remove the last “s” in “providers”	Noted and amended.
96.	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 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.	The steps denoted are necessary for the different types of financial institutions to which the Joint Standard applies.
97.	The South African Insurance Association	8.1.2(a) & 8.1.3	• Paragraph 8.1.2(a) has a typo; the last word must be providers instead of providerss	• Noted, the typo has been deleted. • Inventory is unpacked in 8.1.2(d) above.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
	(SAIA), a representative body of the non-life insurance industry	& 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 8.1.3 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 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 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 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 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.	• 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 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. • 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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			• 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 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	• Cyber resilience capability includes people, process and technology.
98.	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).
99.	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.
100.	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.
101.	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.
102.	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
103.	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.
104.	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.
105.	ASISA	8.2.2 (a)(v)	Not all users who access information assets will work from “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	Noted. The paragraph of the Joint Standard has been amended to include ‘connections’

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			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	
106.	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 something I have, something I am, or something I know.**	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.
107.	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.
108.	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.
109.	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
110.	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.
111.	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.
112.	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.
113.	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.
114.	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	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			requirement in (iv) to further protect via encryption, would the Authority consider reducing this requirement to “prevention” only?	
115.	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;
116. /	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.
117.	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.
118.	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.
119.	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 subject to the same security standards.”	Noted. See response to comment 116 above.
120.	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.
121.	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.
122.	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 available to protect data in storage. Suggest that this section be split to deal with	Noted. See response to comment 120 above.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			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.	
123. 1	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.
124.	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.
125.	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 authentication, device posturing, etc.	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.
126.	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.
127.	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.
128.	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.
129.	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 by third party service providers once it has been returned.	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. 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;
130.	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.
131.	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**	See response to comment 129 above.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			and if this is not possible then there must be secure destruction of storage media containing the financial institution's information**;** 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.	
132.	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.
133.	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.
134.	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 relevant agreements with users"**	Noted. The paragraph has been amended to include 'appropriate' …provisions in the relevant agreements.
135.	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.
136.	Investec	8.2.3(a)(xi)	Suggest adding "with users and all third parties"	Users as defined in the Joint Standard includes third parties.
137.	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.
138.	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.
139.	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.
140.	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." We recommend the changes should not include routine changes e.g. capacity management, etc. but for material changes.	Disagree. Because it is business critical application any change has the potential to disrupt operations or security.
141.	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.
142.	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. .

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
143.	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.
144.	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 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;"	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.
145.	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 .
146.	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.
147.	Standard Bank Group	8.2.5 Network Security (a) (v)	consider isolating internet web browsing activities from its 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 This is worded as a non-mandatory control (consider). Should this be in a standard if it is not mandatory?	See comment 145 above
148.	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).
149.	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.
150.	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 may require amendments to the existing agreements with third party service providers.	Yes. Please consider 8.2.3(a)(iii) above. The financial institution is ultimately responsible even when third parties are providing services.
151.	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'.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
152.	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.
153.	Silica Administration Services (Pty) ltd	8.2.5(vi)	To add: "where possible"	Disagree – this is a minimum requirement.
154.	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…."
155.	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.
156.	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.
157.	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.
158.	Investec	8.2.6a(vii)	It may not be practical for all cryptographic algorithms / keys to be rigorously tested; this 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.	Disagree. It is necessary for the financial institution to test the algorithms in terms of compatibility with the system or whether it is achieving what was intended.
159.	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..
160. 2 3	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.
161.	China Construction Bank	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	See response to comment 160 above.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
	Corporation Johannesburg Branch		/ 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?	
162.	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 expectation that all systems are logged and all logs are retained	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.
163.	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;
164.	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.
165.	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. Noted "exercise' has been removed as it is covered in 'testing'.
166.	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..
167.	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	8.2.3(a)(iv) - Noted. The Joint Standard has been amended as follows:

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			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"**	ensure that sensitive information stored in systems and endpoint devices is encrypted and protected by access control mechanisms commensurate to the risk exposure;
168.	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.
169. 1 1	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.
170.	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.
171.	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, irrespective of the location;** and"	See response to comment 168 above. This is a minimum requirement of the Joint Standard in relation to sensitive information.
172.	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.
173.	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.
174.	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.
175.	ENSAfrica	**8.4.1(e)** A financial institution must implement a clear communication strategy 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 obligation imposed by this section 8.4.1.(e).	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
		impacted by cyber-attacks including details on any recourse available to financial customers.		
176.	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 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.	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.
177.	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.
178.	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.
179.	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:	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			(aa) to share reliable, actionable cybersecurity information regarding threats, vulnerabilities, incidents to enhance defences; and (bb) to receive timely and actionable cyber threat information. **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.	
180.	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.
181.	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). 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.	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
182.	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.
183.	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 knowledge and experience? Currently most banks in the industry are reluctant to share cyber-related event information that could be beneficial to other banks.	See comment 181 above
184.	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
185.	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 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 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."	Insurers should approach the industry bodies to facilitate such information sharing platforms on cybersecurity and cyber resilience. 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.
186. 24	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.
187.	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.
188.	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
189.	BASA	8.6.1 a	**Correct** typo error in “teffectiveness.”	Noted and amended.
190.	First rand Group	8.6.1 a	Correct typo error in “teffectiveness”.	Noted and amended.
191.	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 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.	See response to comment 188 above.
192.	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.
193.	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 expanded to include the above position.	Yes, the requirement includes third party service providers. Also see 8.6.1(b) which relates specifically to third party service providers.
194.	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	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

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			impact the customers as the financial institution will likely increase customer fees to cover the increased overheads which adversely impacts customers.	institution is dire when a cyber incident occurs both to the financial soundness of the financial institution and to financial customers.
195.	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 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.	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.
196.	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.
197.	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.
198.	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.
199.	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
200.	SA Home Loans	8.6.3	Comprehensive penetration testing is an expensive exercise for most institutions. When is the proposed commencement date so that institutions can set appropriate budgets?	The commencement date is approximately 12 months after publication.
201.	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,

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
202.	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.
203.	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 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.	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 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.
204.	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.
205.	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 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".	See response to comment 203 above.
206.	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.
207.	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.
208.	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
209.	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

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
210.	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 years. We respectfully submit that the Authority consider that a financial institution must do one of these tests annually.	See response to comment 202 above.
211.	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.
212.	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.
213.	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.
214.	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 cyber event has disastrous impact on the financial institution and financial customers.
215.	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.
216.	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.
217.	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.
218.	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 they satisfy business policies or rules of the financial institution as well as regulatory and legal requirements. Also see response to comment 201 above.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
219.	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.
220.	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.
221.	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.
222.	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'.
223.	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 involve and adapt.
224.	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.
225.	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.
226.	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.
227.	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.
228.	Two Mountains	8.2.3 a vii	"Adequate processes" what is defined and deemed as adequate? Suggest adding Adequate processes to the Definitions list in Point 4	See response to comment 226 above
229.	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.
230.	Two Mountains	8.6.1 a	Spelling mistake "teffectiveness"	Noted and amended.
231.	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.
232.	Two Mountains	8.6.2 a i	Timely Manner?	See response to comment 198 above.
233.	Two Mountains	8.6.4 a i	Regular – what is deemed as regular? Quarterly / annually?	See response to comment 216 above.
234.	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.
235.	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
236. 9. Cybersecurity hygiene practices				
237.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	9. Cybersecurity hygiene practices (9)	No comment.	Noted.
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 passwordless for authentication (e.g., Windows Hello).	Noted. The paragraph has been amended as follows: (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: (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;

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
244.	BrightRock	9.3	Multi-factor authentication. There has been different 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?	Multifactor authentication is two or more factors.
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 incidentss. 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 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.	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
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 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"~~	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 operating system, database, application, security appliance or network device;~~ and
250.	The South African Insurance Association (SAIA), a representative body of the non-	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?	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
	life insurance industry		Kindly clarify what an "administrative account related to any application" may be. Are administrative accounts on critical systems included in this requirement? 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).	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 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 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 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.	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.
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 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.	See response to comment 254 above.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
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 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”.	The paragraph has been amended to delete the types of devices.
260.	Investec	9.7.1c	Suggest changing “scanning of indicators” to “scanning for indicators of compromise”	(c) 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.
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	See comment 265 above. Independent review can be done internally, and financial institutions do not need to appoint an external party.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			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 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 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.	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
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.
10. Reporting				
271.	Financial Intermediaries Association of	10 – Regulatory Reporting	Clarity is requested on what is meant by 'any' cyber incident.	Noted. The paragraph has been amended.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
	Southern Africa (FIA)			
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.
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 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.	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.
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 material IT and/or cyber incidents". Suggest removing this if there wont be any other reporting requirement relating to this Cyber standard.	Directive 2 will be repealed when the Joint Standard is finalised.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
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, notify the **responsible** Authorit~~ies~~**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."	The paragraph has been amended to require reporting to the responsible authority.
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.	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 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".	The paragraph has been amended to refer to the responsible authority.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
		As read with the definition of "Authorities" under section 1		
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 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 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, <u>with no materiality threshold</u>. 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 <u>of classifying the event as material</u>". This means that an event must only be reported within 24 (twenty four) hours <u>of classifying the event as "material"</u>, not that the event must be 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 <u>incident</u> would fall within the meaning of an "<u>event</u>" 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.	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 • 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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
			In the third instance, if it was rather intended that a financial institution should report an 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 "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.	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. 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, 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.	The notification template will be published for comment when the Joint Standard is published for formal consultation.
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	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
		reporting for this Joint Standard		
291. 11. Short title				
292.	OUTsurance Holdings Limited, OUTsurance Insurance Company Limited and OUTsurance Life Insurance Company Limited	11. Short title	No comment	Noted.
293.	Aurora Insurance Company	11.1	Duly Noted.	Noted
294.	The South African Insurance Association (SAIA), a representative body of the non-life insurance industry	Short title	No Comment	Noted
General comments				
295.	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.
296.	Nedbank Limited	General comments	Participated in the BASA process	Noted.
297.	Equity Express Securities Exchange (Pty) Ltd	General comments	None	Noted
298.	The Federated Employers Mutual Assurance Company (RF) (Pty) Ltd	General comments	None	Noted.
299.	The Cape Town Stock Exchange	General comments	None	Noted.
300. 3 3	Integrity Retirement Fund Administrators (PTY) Ltd		None	Noted.
301.	Habib Overseas Bank Limited	0.All sections	Agree with the proposed wording	Noted.
302.	Clientele Limited	0.None	None	Noted.
303.	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.

No	Reviewer	Draft standard reference Section and paragraph	Comment/ Issue	Response
304.	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.
305.	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.
306.	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.
			Statement of need	
307.	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.
308.	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 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 practical day to day regime is required.	The proposed Joint Standard outline the minimum requirements and standards to be implemented by the regulated entities. The Joint Standard aims to 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.