



SOUTH AFRICAN RESERVE BANK
Prudential Authority

Comments received on the Draft Determination of the notification template in terms of Joint Standard 1 of 2023 – IT Governance and Risk Management for Financial Institutions and Joint Standard 2 of 2024 – Cybersecurity and Cyber Resilience Requirements for Financial Institutions as at the close of the commenting period on 05 October 2025

October 2025

Contents

List of commentators.....	3
Comments received on the draft determination.....	4
Comments received on the reporting template.....	15

List of Commentators

NO	NAME OF ORGANISATION	CONTACT PERSON AND CONTACT DETAILS
1.	ASISA	Johann Van Tonder
2.	Vodacom Insurance Company and Vodacom Life Assurance Company	Siyabonga Vumijojo
3.	Standard Insurance Limited	Sue Chetti
4.	Sanlam Developing Markets Limited	Akisha Harilal
5.	Banking Association South Africa (BASA)	Mcdonald Madeyi
6.	OUTsurance	Kurayi Matsika
7.	Institute of Retirement Funds Africa NOC	Wayne Hiller van Rensburg/Nancy Andrews
8.	ITLawCo	Nathan-Ross Adams

COMMENTS ON THE DRAFT DETERMINATION					
No	Reviewer	Draft reference paragraph	Determination section and	Comments/ Issue	Response
1.	ASISA	General		The Regulators are requested to provide clarity regarding the reporting of incidents that impacts various business units (providing different types of financial services) within one financial services group - it could be multiple licenses that can span across both the PA and the FSCA. Does the reporting portal accommodate for one report incorporating all the impacted business units within the group, or is the expectation for separate reports for each license? If the latter, it is proposed that the Regulators consider that one report be submitted, including a list of all business units (licenses) and that both the PA and FSCA have access to the information.	Noted. At this stage it is not possible since the Prudential Authority and the Financial Sector Conduct Authority (FSCA) (hereinafter referred to as the Authorities where appropriate) do not have a joint platform. This is being considered for future implementation. Based on the determination, the notification must be sent to the responsible authority for the legislation in terms of which the financial institution is licensed. The PA and the FSCA will then share the information between each other, where necessary.
2.	ASISA	General		It is proposed that the Regulators consider digitizing the form for online completion and submission. Perhaps a web-based portal with validation and workflows – allowing different persons within the financial services company access. The motivation for this is that, at the initial point of reporting the incident, all information might not be available, but as the investigation continues and more information becomes available, the online form can be updated with the new information. It will further help to reduce manual errors and with response times.	Please note the Authorities are currently at an early stage in the digitisation journey and will work toward streamlining and reducing duplication of efforts. It is also important to recognise that different financial institutions under separate licensing regimes may have varying requirements. Currently the PA receives submissions through the Umoja Portal. The FSCA will utilise the Joint Standards Submission Portal for this purpose, with the portal becoming effective/operational on 01 September 2026.
3.	ASISA	Paragraph 4		Members request an implementation period to ensure alignment of their systems and procedures to comply with the determination and thus request that the notification template becomes effective on a date six months after it is published in final form.	Disagree. There is no development required at this stage from financial institutions, as this is a manual process. Financial institutions are expected to comply with the requirements of the Joint Standard on IT Governance and Risk Management from November 2024 and the Joint Standard on cybersecurity and cyber resilience from June

				2025. Directive 2 of 2019 pertaining to banks and GOI 3.2 relating to insurers still require material incidents to be reported and such instruments will be repealed once the determination becomes effective.
4.	Vodacom Insurance Company and Vodacom Life Assurance Company	N/A	We acknowledge receipt of the proposed template for reporting IT and Cyber incidents. While we appreciate the Authority's efforts to standardise incident reporting, we would like to request additional time to assess the template requirements in relation to our existing internal processes and obligations. Currently, our organisation has processes to report incidents—particularly those involving the leak of personal information—to the Information Regulator in line with regulatory requirements. To ensure alignment and avoid duplication or inconsistencies across reporting channels, we need to evaluate how the proposed template integrates with these established procedures. Once this assessment is complete, we will be in a better position to provide constructive and informed feedback on the proposed reporting framework. These processes cover different teams, including IT, Privacy, and Cybersecurity, and require engagement across these teams; therefore, we request an extension until 31 October 2025.	Disagree. The Authorities are of the view that sufficient time was granted for input, especially since the notification template was included in the public consultation process for both Joint Standards.
5.	ABSA	3.1(a)	What is the process for submission if the Umoja portal is not available.	It will be dealt with on a case-to-case basis. The PA's first point of contact is the frontline teams.
6.	ABSA		Who defines what is a material IT/Cyber incident?	The financial institution defines materiality as outlined in both Joint Standards.
7.	ABSA		More clarity is needed on what is a Cyber Incident, example if no system was compromised and or security settings changed, but data was leaked by a staff member that had the access to the information but abused his/her access is this a Cyber Incident or a Fraud Incident?	As defined in the Joint Standards a cyber incident means a cyber event that (a) jeopardises the cybersecurity of an IT system or the information processed, retrieved, stored or transmitted by the system; or

				(b) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. Based on the example provided, security policies and procedures were violated and thus the incident will be classified as material.
8.	ABSA	3.2	Assuming that there will be an initial upload and then a more complete upload later? Does the reporting template need to be maintained on the Umoja toolset, or will multiple versions of the same sheet be uploaded to the Umoja portal?	If there are any updates, then additional versions of the same sheet should be uploaded to the Umoja portal.
9.	ABSA	General Comment	Is there an intention to create an online submission format for the notification ie. System based submission as opposed to uploading an Excel document?	Yes, the Authorities are working on digitalising the notification template.
10.	Standard Insurance Limited	N/A	N/A	Noted.
11.	Sanlam Developing Markets Limited	Definitions	No comment	Noted.
12.	Sanlam Developing Markets Limited	Determination of form of notification	No comment	Noted.
13.	Sanlam Developing Markets Limited	Manner and time frame of notification	No comment	Noted.
14.	BASA	General	1. The current regulatory landscape contemplates 4 separate reporting requirements namely: a. Banks Act Directive 2 of 2019 - Reporting of material information technology and/or cyber incidents b. FSCA & PA Joint Standard 1 of 2023 - IT Governance and Risk Management for Financial Institutions, 2023	1. Where a bank reports in terms of the Joint Standards, there will be no need to report in terms of the Banks Act Directive 2 of 2019. This Directive will be repealed once the Joint Determination is finalised. The bank must decide whether the material incident is cyber or IT related and report under the respective

			c. FSCA & PA Joint Standard 2 of 2024 - Cybersecurity and Cyber Resilience requirements for Financial Institutions, 2024 d. Notice 4835 of 17 May 2024 - Directive 1 of 2024: Cybersecurity and Cyber-resilience within the National Payment System 2. It is unclear if this joint determination which specifies that it is issued to stipulate reporting requirements in terms of (b) and (c) seeks to replace (a) which if remains, will be a duplication. Clarity is requested from the regulator in this regard. 3. Furthermore, (d) includes a requirement for payment institutions or operators to report material cyber incidents to the SARB within 24 hours and provide a report to the SARB within 48 hours of the attack including the same information requested by the joint determination. 4. As indicated in our previous engagements with the SARB PA, there is a clear inconsistency in timing of reports containing the same information between the SARB NPSD and the SARB PA and FSCA. 5. The Financial Sector Regulation Act S76 (1) establishes a statutory duty between the SARB and other financial role players including the FSCA, SARB PA, NCR and FIC to cooperate and collaborate when performing its functions in terms of financial sector laws. However, the fulfilment of this requirement is not evident through recent publications including the requirements cited above. Clarity in this respect is sought to ensure legal certainty in application of the specified requirements.	Joint Standard; if it is both, then once notification referencing both Joint Standards is acceptable. 2. Yes, the determination will replace directive 2 of 2019, which will be repealed once the determination is issued. 3. It is key to note that this is a requirement from a different Regulator and must be complied with in terms of the requirements stipulated. 4. Noted, as per 3 above. The Authorities will engage with the National Payment System Department to create consistency, where possible. 5. Please refer to response to sub-comment 4 above.
15.	BASA	General	For financial groups that consist of various types of financial institutions, does the reporting portal accommodate for one report incorporating the impacted financial institutions within the group? Alternatively, is the expectation for separate reports for each licence in light of the fact there will be an initial upload and then a more complete upload later? Does the reporting template need to be maintained on the Umoja portal, or will multiple updated versions of the same sheet be uploaded to the Umoja portal? What is the process if the Umoja Portal is not available?	Currently, the requirement is that every affected financial institution must notify the responsible Authority for the legislation in terms of which it is licensed. This will be either the PA or the FSCA. Please also see the response to comments 8 and 5 above.

16.	BASA	Paragraph 2	Reference is being made to the “Reporting of material IT and/ cyber incident template” however the template/Annexure B is referred to as “Material Incident Report Form for IT Governance and Risk Management, and Cybersecurity”. It would be prudent to refer to the document consistently to ensure certainty in referencing and application thereof.	Noted. The necessary amendments have been made to ensure consistency to the reference of the reporting template.
17.	BASA	Paragraph 2.1	This paragraph is not clear as to what the subject matter is. We would propose the following amendment for clarity: <i>The Authorities have determined the form, manner and information to be notified to the responsible Authority by a financial institution when an incident is classified as a material IT and/or cyber incident, in terms of paragraph 15.1 of Joint Standard 1 of 2023 – IT Governance and Risk Management for Financial Institutions and paragraphs 9.1 and 9.2 of Joint Standard 2 of 2024 – Cybersecurity and Cyber Resilience Requirements for Financial Institutions, as set out in this Schedule and the ‘Reporting of material IT and/or cyber incident’ template (template).</i>	Disagree. Please note that the determination is catered for in the cover page of the Joint Notice.
18.	BASA	Paragraph 4	Member banks request an implementation period to ensure alignment of its systems and procedures to comply with the determination and thus request that the notice takes place on a date six months after the notice is published in final form.	See response to comment 3 above.
19.	OUTsurance	Tab 1 – Immediate notification	1. Does 24 hours refer to business hours? 2. Will the 24 hours apply from identifying the incident or from when the incident has been classified as material? 3. We recommend that 24 business hours be afforded, instead of 24 ordinary hours for notification as further investigation is at times required in order to establish whether a cyber incident is classified as material or not.	1. No, it refers to ordinary 24 hours from the time the incident is classified as material. The 24 hours is the maximum time within which the notification must be made; however, the material incident can be reported sooner if the information is available. 2. The 24 hours applies from the time that the incident has been classified as material. 3. Disagree. Financial institutions are only required to provide certain information within 24 hours; thereafter, the institutions will be afforded further opportunities to provide updates.

20.	OUTsurance	Tab 5 - Sensitive customer data leaked?	1. For clarity, we recommend that what constitutes sensitive customer data be clarified. Does sensitive customer data refer to personal information as defined in the Protection of Personal Information Act or to any information deemed sensitive by the institution?	Sensitive customer data must be read as 'sensitive information' which is defined in the Joint Standard 2 of 2024 - Cybersecurity and Cyber Resilience. Sensitive information means information or data were loss, misuse, unlawful disclosure or unauthorised access to or modification of could adversely affect the public interest or a financial institution or the privacy to which persons are entitled.
21.	Institute of Retirement Fund Africa NOC	1. Definitions: "material incident"	Comment: The definition of a "material incident" is overly broad and may lead to uncertainty for pension funds and their administrators. It is unclear whether a cyber breach affecting a single participating employer would qualify as a material incident, or whether administrators are required to report every ransomware attempt regardless of whether data or services are actually disrupted. Recommendation: We recommend the inclusion of proportionality wording to establish materiality thresholds that are specific to the type of financial institution. For pension funds, a narrower trigger should be considered, such as where fund data integrity, member benefits, or contributions are materially compromised. The Authorities should consider providing sector-specific guidance on materiality thresholds or a principles-based assessment framework.	Disagree. The Joint Standards are principle based and considers proportionality and risk profile of the supervised institution, based on the nature, size and complexity of the financial institution. The existing principle-based framework provides sufficient flexibility for financial institutions to exercise professional judgements. The definition of "material incident", amongst others, indicates that the incident caused a disruption in the business activity of an institution and the incident has or is likely to have a widespread impact on operations or services to customers. The responsibility for the classification of a material incident rests with the financial institution and the definition provides some guidance on what constitutes materiality. The financial institution will also have to measure the impact and the severity thereof in terms of their own business practices and determine whether reporting is needed.
22.	Institute of Retirement Fund Africa NOC	1. Definitions: "Umoja Portal"	Comment: The requirement for pension funds and administrators to submit notifications via email raises concerns about security, tracking, and potential for technical failures (e.g., emails being delayed, lost, or	Please note that the FSCA has resolved to establish a dedicated submission portal, namely the Joint Standards Submission Portal, which is scheduled to be

			blocked by spam filters). There is no automated acknowledgment of receipt or audit trail. Recommendation: We recommend that the Authorities provide an alternative, secure submission mechanism, such as a dedicated portal, for all financial institutions. If email submission is retained, the Authorities should implement automated acknowledgment of receipt and provide clear guidance on encryption and security requirements.	effective/operational on 01 September 2026. With regards to “acknowledge of receipt”, it is envisaged that the portal will have a report / audit trail capability. In addition, the portal will upon submission by the regulated entity issue automated “notification / acknowledge of receipt”.
23.	Institute of Retirement Fund Africa NOC	3. Manner and time frame of notification	Comment: Most pension funds have no direct IT systems and delegate IT functions to the appointed administrators. The draft requires the governing body/board of trustees to ensure compliance, even where they lack operational control. It is unclear whether both the fund and the administrator are required to submit reports for the same incident, leading to potential duplication and regulatory burden. Recommendation: We recommend that the Authorities clarify that where IT and cyber functions are fully delegated to the administrator, the administrator's notification will suffice, provided that: (a) appropriate contractual arrangements are in place requiring the administrator to notify the Authorities and the Fund's board of trustees; (b) the board is informed within a reasonable timeframe; (c) the board retains oversight responsibility for incident response procedures; and (d) the administrator's notification clearly identifies the affected pension fund(s).	Disagree. The governing body of the financial institution retains the ultimate fiduciary duty to oversee the operations. The financial institutions are responsible for outsourced activities; and the responsibility and accountability cannot be delegated to the service provider. Contractual arrangements with the service provider must be clear on the requirements of the Joint Standard and reporting of any incidents to the financial institution. Furthermore, the recommendation does not align with the fiduciary duties imposed on the governing body of the financial institution. Therefore, the Authorities disagree with the approach to allow an Administrator's or any other delegated/Third-Party's or outsourced entity's notification to suffice as “proxy” for regulated/supervised financial institutions' reporting obligations, as this proposal misaligns/contradicts the legal principle in the Joint Standards that vest the governing body with the ultimate fiduciary duties.
24.	Institute of Retirement Fund Africa NOC	3.2 Time frames	Comment: The notification template requires highly technical and forensic-related information (root cause, attack surface, entry vector) that may be difficult for pension funds, especially smaller funds with limited resources, to provide within the stipulated time frames. Immediate and comprehensive notification may be impractical, and	Noted. The notification does set reporting stages being: (1) Immediate notification within 24 hours after classifying the incident as material.

			requiring premature reporting of incomplete information serves neither the Authorities nor the regulated entities. Recommendation: We recommend a three-stage reporting structure: (1) Immediate notification within 24-48 hours with basic details (detection date, preliminary classification, affected systems, initial response); (2) Interim update within 14-21 days with preliminary findings on impact and remediation actions; (3) Final report within 60-90 days or upon completion of investigation with comprehensive root cause analysis and lessons learned.	(2) Interim update within 14 calendar days from the date of notification. (3) Final report as agreed with the Authorities. The question of technical and forensic information, rests purely in the intent and depth of the financial institution's enquiry to the incident or cyber event. The reporting stages set by the Joint Standards are appropriate as they assist the Authorities in being pro-active and pre-emptive, to monitor risks that may arise.
25.	Institute of Retirement Fund Africa NOC	3.2 Time frames	Comment: Smaller financial institutions may not have the capabilities in place to comply with the time frames. The South African pension fund industry is highly diverse, ranging from large umbrella funds to small employer-sponsored funds with minimal administrative infrastructure. Recommendation: We recommend that the Authorities provide for a grace period or simplified reporting pathway for smaller pension funds (e.g., those with fewer than 500 members or assets under management below a specified threshold), or publish guidance specifically tailored to smaller funds with reduced technical detail requirements and longer timeframes.	Noted. However, the current reporting requirements are reasonable for smaller financial institutions. Also see response to comment 24 above. The proportionality principle contemplated in the Joint Standards and the notification requirements and timelines did consider the nature, complexity, size of the financial institution. For instance, for a "small financial institution", a breach or material event may harm its customers or members, this will be a conduct issue, thus it is commensurate with the actual "conduct risk" however it may not be systemic or have contagion effects. Therefore, all entities, even the smaller entities should be able to do "immediate notification" within the specified timelines.
26.	Institute of Retirement Fund Africa NOC	3. Details of the Incident (Row A8)	Comment: Financial institutions already have overlapping breach notification requirements under POPIA. The template asks whether notification has been sent to other Authorities (e.g., Information	Noted. Although the template asks about notification to other Authorities, each authority is independent, thus supervised entities should report as per sectoral laws.

			Regulator, NPSD), but does not clarify whether institutions may cross-reference reports already filed with another Authority. Recommendation: We recommend that the Authorities clarify that where a pension fund or administrator has already submitted a notification to another regulator (e.g., the Information Regulator under POPIA), they may cross-reference or attach a copy of that notification in their submission to the FSCA and Prudential Authority, provided that it contains substantially the same information. This would reduce duplication and administrative burden.	In addition, notifications required under these Joint Standards may not be substantially the same as others required by other regulators. Moreover, it is important to recognise independence of the regulators. Reliance on reports submitted to other regulators introduces third-party leg and information filter. Notification templates must be completed according to the requirements sets in the template. Certainly, there is value in cross-referencing / leveraging an already existing report which may contain substantially same information.
27.	Institute of Retirement Fund Africa NOC	4. Short title and commencement	Comment: The draft currently states "MM-DD-2025" without a specific commencement date. A transitional period is necessary to allow all financial institutions to develop the capabilities, systems, processes, and contractual arrangements required to comply with the new reporting requirements. Recommendation: We recommend that the Authorities specify a commencement date that is at least six months after the publication of the final determination, and provide for a transitional period during which the Authorities adopt a more flexible approach to enforcement, focusing on engagement and education rather than punitive action.	See response to comment 3 above.
28.	Institute of Retirement Fund Africa NOC	General: Guidance and Definitions	Comment: The notification template contains numerous fields with dropdown menus or free-form text entry, but provides limited guidance on how to complete these fields. Terms such as "preliminary incident classification", "origin", "cause of incident", "category of attackers", and "entry vector" are technical in nature and may be interpreted differently by different institutions. Recommendation: We recommend that the Authorities publish comprehensive guidance notes to accompany the notification template, including: (a) definitions of key technical terms; (b) examples of how to classify incidents; (c) illustrative scenarios showing how different types of incidents should be reported; and (d) clarification of ambiguous	The Authorities may consider developing guidelines in the near future. Such possible guidance may possibly set out the Authorities expectations on the application of the Joint Standards.

			terms. This guidance should be developed in consultation with industry participants.	
29.	ITLawCo	General – “Material incident”	The Draft relies on institutional discretion to define “materiality”. For clarity and consistency, FSCA should issue objective thresholds (e.g., >500 clients impacted, >R5m financial loss, >4 hours downtime), similar to EU DORA. Explicit thresholds will reduce under- and over-reporting.	Noted; however, the Joint Standards are principle based and considers proportionality and risk profile of the supervised institution. What may be material to one financial institution may not be to another. The classification falls within the responsibility of the financial institution.
30.	ITLawCo	Reporting Timelines	The 24-hour initial reporting requirement is ambitious but globally aligned (e.g., DORA: 4–24h, MAS: 1h/24h, SEC: 4 business days). FSCA should provide guidance on “minimum facts” expected in the 24h notice (e.g., detection method, affected system, preliminary scope) to avoid rushed or speculative submissions.	See response to comment 24 above. Refer to the “cover page” tab for details.
31.	ITLawCo	Submission Mechanism	Currently, Umoja Portal applies to some institutions while others submit via email. Dual channels risk fragmentation. We recommend FSCA roadmap toward a unified digital submission hub for all institutions.	Noted. See response to comment 2 above.
32.	ITLawCo	Supervisory Feedback	The Draft does not commit to supervisory feedback. International practice (EU ESAs, CISA) includes anonymised sectoral reporting. We recommend FSCA publish anonymised incident trends and sector alerts to strengthen collective resilience.	Supervisory feedback is provided to industry forums however as the process matures and more data is available from incidents, sectoral reporting may be considered.
33.	ITLawCo	Proportionality	The Draft applies uniformly to all institutions. We recommend tiered obligations: systemic banks → full reporting, small FSPs → lighter requirements, to balance regulatory burden with systemic risk.	Disagree. The Joint Standards are principle based and considers proportionality and risk profile of the supervised institution, depending on the nature, size and complexity. What is a material incident in one firm may not be a material incident to another. The Authorities have a mandate regarding the financial soundness (PA) and customer protection (FSCA) regarding each financial institution.

				In addition, the Joint Standards apply consistently across all impacted sectors, with scope for sector-specific considerations.
34.	ITLawCo	Confidentiality	Early reports may contain sensitive or incomplete data. FSCA should confirm confidentiality protections and allow iterative updates without penalty if initial facts change.	The information submitted to the Authorities is handled based on its classification and in terms of the Financial Sector Regulation Act, 2017. The Authorities handle information and data through the framework of statutory confidentiality and secrecy and limited purpose and disclosure. Authorities ensures that there are appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of the information, and unlawful access to or processing of the information. Financial institutions are discouraged from making changes to the initial submission. Supervised institutions have the opportunity to provide further updates in subsequent reporting stages.
35.	ITLawCo	Implementation & Testing	We recommend FSCA encourage annual cross-functional simulations (IT, legal, compliance, board) to test readiness for the 24h rule. A pilot phase with selected institutions could also help identify practical gaps before full rollout.	Noted. The Authorities have observed that many supervised entities are already conducting simulation exercises which are in line with the requirements of the Joint Standards.

COMMENTS ON THE REPORTING TEMPLATE					
No	Reviewer	Name of Sheet	Row and Column No	Comment	Response
36.	ASISA	Cover Page	General	Provision should be made for additional or outstanding information to be provided in the “details of incident” and “cyber incident info” sheets in subsequent updates. Similarly, throughout the investigation of the event there may be instances where the information previously disclosed on the notification template changes and as such financial institutions must have the opportunity to amend their responses prior to the conclusion of the final investigation. This is aligned with proposal in comment 2 in Section B.	See responses to comment 34 above.
37.	ASISA	Cover page	Rows 11 & 12, Column B	The experience of members from incidents as well as simulation exercises, carried out as part of cyber incident readiness training, have indicated that it takes substantial resources and time to contain material incidents. Consequently, the first day will often be taken up with efforts aimed at identifying that an incident has taken place, containing the incident to prevent further harm and assessing materiality. The amount of information available within 24 hours is therefore often sparse and, in some respects, incorrect as no validation processes will have taken place. There is a risk that members may need to split the focus of their resources from containment measures to information gathering to enable reporting. This could be to the detriment of impacted customers and other affected stakeholders. ASISA members therefore propose the following restatement of Annexure A: • immediate notification within 24 hours with a description of the event and, on a best-effort basis, all information which is known at the time; • subsequent update within 72 hours with all the available information as indicated in Column C of Rows 11 & 12. In this regard, further refer in proposal in comment 2 in Section B. It is further proposed that a unique descriptor be added to distinguish multiple submissions relating to the same reported incident, as well as	The Authorities are of the view that the individuals reporting the incident to the Authorities should not be the same individuals who are involved in containing the incident, clearly ensuring segregation of duties, and not hindering the process of containment. Furthermore, information submitted to the Authorities is handled based on its classification. Financial institutions are discouraged from making changes to the initial submission. Supervised institutions have the opportunity to provide further updates in subsequent reporting stages. The current reporting requirements are responded to in comment 24. Each incident is evaluated based on its merit, every incident submitted on Umoja has a unique identifier. From an FSCA perspective and in terms of the dedicated mailbox folder which has been created for notifications, the FSCA will be in a

				reporting on multiple incidents that might occur close to each other and while investigations on each are still ongoing.	position to accordingly handle the submissions made on a case-by-case basis.
38.	ASISA	Cover Page	Row 13, Column B	It is proposed to change the 14 calendar days to 14 business days given the extent of the details required in Sheet 5 (Impact of the incident).	Disagree, the Authorities are of the view that the current reporting requirements are sufficient Please see response to comment 37 above on the reporting requirements.
39.	ASISA	Details of incident	New Row (after Row 9)	The date of incident detection might be different from when it is determined that the incident qualify as “material”. It is therefore proposed to add an additional row which allows for the provision a reason for the delayed reporting.	Noted. Notification within 24 hours after classifying the incident as material is the requirement Financial institutions have an option to provide additional information on column C.
40.	ASISA	Cyber incident info	Row 11, Column A	It is proposed to add the words “of the threat” after the word “Origin”.	Noted. The reporting template has been amended to read “Origin of the threat”.
41.	ASISA	Cyber incident info	Row 15, Column B	It is proposed to add “unknown” as an option on the drop-down list as this information may not be known at the initial time of notification.	Noted. The reporting template has been amended to include “Unknown” as an option.
42.	ASISA	Impact of the incident	Row 9, Column A	The Regulators are requested to provide clarity on what the focus is with the question “<i>Was there any unauthorised release of data</i>”. It could be one or more of the following: • that unauthorised access to data was obtained • that the data obtained (unauthorised) was released or published (either publicly or on the dark web) • that the data obtained (unauthorised) and published, was acquired by an authorised party • that the accessed unauthorised data was subsequently recovered	Noted. The Authorities have amended the reporting template to split the question into two and rephrased the wordings to read: “Was there any unauthorised access of data?” and “Was there any intentional/unintentional release of data?”. The questions are now row 9 and 10.
43.	ASISA	Impact of the incident	Row 10, Column A	The Regulators are requested to provide clarity on the meaning of “<i>sensitive customer data</i>”. • Does it refer to special personal information as defined in POPIA or does it have a broader meaning, or • Does it refer to “sensitive information as defined in the Joined Standard on Cybersecurity and Cyber Resilience Requirements.	See response to comment 20 above. Both Joint Standards must be read in conjunction.

				Does it refer to “sensitive or confidential information as defined in the Joint Standard on IT Governance and Risk Management A further question is what about sensitive (strategic) information that relate to the financial institution?	
44.	ASISA	Impact of the incident	Row 16, Column A	The Regulators are requested to provide clarity on “ <i>did any claims arise due to the incident</i> ”. Does it refer to claims from customers or insurances claims by the financial institution.	Noted. This has been reworded to “Have any claims been lodged against the financial institution as a result of the incident”. The question is now row 17.
45.	ASISA	Impact of the incident	Row 16, Column B	ASISA members are concerned that this question could not be answered completely and accurately within the required 14-day reporting time, as there may be instances where claims may not have taken place yet. It is proposed to add a third option “not at present” or “still to be determined” to the drop-down list.	Agreed. A third option was added being “Still to be determined”. The question is now row 17.
46.	ASISA	Impact of the incident	Row 20, Column A	The Regulators are requested to provide clarity on what is meant with “ <i>Are there any provisions in place for enhanced customer service?</i> ”	The question relates to whether the financial institution has enhanced its customer service to be able to deal with issues arising from the material incident. It extends to the Treating Customers Fairly (TCF) outcomes and it speaks to operational measures in places, including communication channels, hotline, established helpdesks, etc.
47.	ASISA	Impact of the incident	Row 29, Column B	It is proposed to make the response in Column B a drop-down (with a yes/ no), followed by details if the answer is yes.	The template has been updated accordingly including provision for additional information on column c. The question is now row 30.
48.	ASISA	Impact of the incident	Row 43, Column A	It is proposed to replace the word “ <i>police</i> ” with “law enforcement”.	Agreed. The template has been updated accordingly.
49.	ASISA	Impact of the incident	Row 43, Column C	It is proposed to add the words “if applicable / available” after the word “report”.	Agreed. The template has been updated accordingly.

50.	ASISA	Impact of the incident	Rows 47 – 49, Column B	It is proposed that the Regulators reconsider the value ranges and to include broader upper limits.	Noted. The Authorities have removed the ranges and amended the field for the input of free text. The questions are now 45, 46 and 47.
51.	ASISA	Impact of the incident	Row 50, Column A	Practically it might not be possible to know this information within the required 14-day reporting as the time for recoveries can be extensive. It is proposed to add a third option “not available” to the drop-down list.	Agreed. The template has been updated accordingly. The question is now row 48.
52.	ASISA	Impact of the incident	Row 50, Column C	It is proposed to add “Please provide more details” in this column.	Agreed. The template has been updated accordingly.
53.	ASISA	Impact of the incident	Row 53, Column A	Given that formal training may not always be necessary it is proposed adding the words “or awareness” after the word “ <i>training</i> ”.	Noted. The question “Are there measures in place for future training sessions based on lessons learnt from this incident?” has been removed.
54.	ABSA	Contact Details	9 column B	Is this the date of discovery or the date of notification	This is the date of notification (this is for future reference), the discovery date can be found on the details of the incident, column A row 9.
55.	ABSA	Cyber Incident Info	11 column B	If the attack was against one of our Third Parties caused by their staff clicking on a link – would you classify this as Internal or External?	External, however it will also depend on the source i.e. whether it is an insider threat or external attacker. The attack would be categorised as internal if the third party was physically stationed within the financial institution or the third party was working on the financial institution’s network/systems.
56.	ABSA	Impact of the incident	9 column B	If a person accidentally shared data to a person that it was not meant to be shared with – is this classified as unauthorised release of data?	See response to comment 42 above.
57.	ABSA	Impact of the incident	10 column A	Please define what is sensitive customer data	See response to comment 20 above.
58.	ABSA	Details of incident	10 column A	Materiality Thresholds - The material incident report form (form) relies on a broad definition of “material incident” as one with severe and widespread impact on operations, customer services, or financial	The financial institution must consider ‘materiality’ as outlined in both Joint Standards.

				stability. There is no quantitative threshold or illustrative examples to guide borderline cases. This may lead to inconsistent classification with financial institutions. Suggest that there be predefined criteria for what constitutes a material incident and how to assess it. A severity classification matrix would help with this. Allowing banks to specify their own criteria may lead to inconsistencies.	The Joint Standards are principle based and considers proportionality and risk profile of the supervised institution. The Authorities may consider through supervisory observations releasing high level information on notifications sent to the Authorities.
59.	ABSA	Details of incident	16 column A	Suggest that any incident classification be done via a incident severity matrix. Could potentially collapse this with the field in row 10 column A.	Disagree. Financial institutions use different approaches for their severity assessment, and the provided matrix is broad enough to cover all financial institutions.
60.	ABSA	Cyber incident info	14 column A	Would suggest type of attack be a dropdown with a predefined list of attack types. Different organisations may have a different understanding of incident classification and attribution and this may lead to inconsistencies.	Noted. Attack types, however, are continuously evolving, the template may require continuous updating to keep up with the changing threat landscape. The template, therefore, has a free text field to allow the financial institution to capture the details of the attack type.
61.	ABSA	Impact of the incident	16 column A	What claims are being referred to? Are these customers claims or insurance claims?	Noted. The question “ <i>did any claims arise due to the incident and what was the outcome</i> ” have been amended to “have any claims been lodged against the financial institution as a result of the incident”.
62.	ABSA	Impact of the incident	18 column A	The question almost seems to be a pre-incident type question. FIs should have these measures in place before an incident. Perhaps consider changing the question to be incident specific or remove.	Disagree. Possible measures might exist, but the measures implemented will be determined by the financial institution on a case-by-case basis depending on the circumstances.
63.	ABSA	Impact of the incident	30 column A	Media coverage may on occasion not be immediate. We have seen media engagement on issues up to 8 months after the incident. How will the reporting account for that scenario?	Noted. It is the expectation of the Authorities, however, is to understand whether there was any immediate media coverage.

64.	ABSA	Impact of the incident	34 column A	What is meant by “factors”. I see this is free text. Could this please be more specific, or a drop down?	Noted. The templated has been amended to read: “What caused the incident to occur”. The question is now on row 35.
65.	ABSA	Impact of the incident	35 column A	Seems unnecessary to indicate that an incident response plan has been activated. Reporting a material incident would imply that an incident response plan was activated.	Disagree. The question must be read in conjunction with 36 and 37 which covers Business Continuity Management.
66.	ABSA	Impact of the incident	38 column A	Institutions must confirm whether the incident has been escalated to the board or relevant governance structures. There is no clarity on what qualifies as “escalation” (e.g., formal board meeting vs. email notification), nor on timing expectations for such escalation.	The Authorities do not prescribe the communication channel, the usual form and manner which the financial institution uses to escalate matters, will suffice.
67.	ABSA	Impact of the incident	40 and 41 column A	It is good that there is a distinction between resolution and recovery. Perhaps prudent to provide a definition of resolution and recovery in the context of the template for consistency purposes.	Resolution in the context of the reporting template refers to the solution that was applied to the incident. Recovery refers to the ability of the organisation to revert to normalcy after the incident.
68.	Standard Insurance Limited	5. Impact of the incident	n/a	This sheet contains field requirements that are largely related to a Cyber/Security incident, as opposed to a general IT incident. Can this sheet be split into two tabs: • One applicable to Cyber/Security incidents • One applicable to other IT incidents	To avoid duplication and complexities, the Authorities combined the two sheets as some questions are applicable to both IT and cyber incidents.
69.	Standard Insurance Limited	3. Details of incident	n/a	In meeting the 24-hour notification requirement, and during this 24-hour timeline, we may not always know the full materiality. Could there be an indicator to reflect that this is a cautionary notice? The full 14-day update (Sheet 5. Impact of the incident) may then not be relevant to provide in the full detail required if it is indeed confirmed that the notification was cautionary (and not material).	Noted. However, the current reporting requirements are outlined. See response to comment 24 above.

70.	Standard Insurance Limited	n/a	n/a	At the moment, we use the Form IF046 - Notification of major disruptions to risk profile to notify the PA on IT incidents within 24 hours. Our understanding is that once effective, the new templates will be used for IT & Cyber Security incidents, and the existing Form IF046 - will only be used for major disruptions that has the potential to have a material impact on the insurer's risk profile or affect its financial soundness or security requirements (<i>and not IT/Cyber incidents</i>). We will appreciate any guidance or confirmation on this approach.	Agreed. The IF046 will continue to be used for other major incidents other than IT and Cyber.
71.	Sanlam Developing Markets Limited	Cover page	All rows and columns	No comment	Noted.
72.	Sanlam Developing Markets Limited	Contact Details	All rows and columns	No comment	Noted.
73.	Sanlam Developing Markets Limited	Details of the incident	All rows and columns	No comment	Noted.
74.	Sanlam Developing Markets Limited	Cyber Incident Info	All rows and columns	No comment	Noted.
75.	Sanlam Developing Markets Limited	Impact of the Incident	All rows and columns	No comment	Noted.
76.	BASA	Cover page	General	Paragraph 3.1.(a) of the Notice – manner of notification – banks: requires that the template must be completed and submitted on the Umoja portal and provides a selection path. The template does not include the same instruction, and it is therefore requested that it is included on the cover page to ensure application.	Disagree. The submission methods are different for the two Authorities. Umoja is only utilised for the PA. The manner of notification is contained in the Determination.

77.	BASA	Cover page	General	For ease of reference, please include links to the different Joint Standards as well as as be clear which Authorities need to be notified.	Disagree. The Joint Standards have been published on the Authority's respective websites. Notification is to the responsible Authority in terms of which the financial institution is licensed or registered as clearly indicated in the Determination.
78.	BASA	Cover page	General	In respect of the 24-hour reporting period, we request that we extend that to 48 hours. This will enable us to answer the questions under tab 4 with more comprehensive information. Alternative suggestion: BASA member banks support the important oversight role which is played by the Authorities in managing material IT and Cyber Incidents. The experience of the teams as well as simulation exercises carried out as part of cyber incident readiness training have indicated that it takes substantial resources and time to contain an incident of this nature. Consequently, the first day will often be taken up with efforts aimed at identifying that an incident has taken place, containing the incident to prevent further harm and assessing materiality. The amount of information available within 24 hours is therefore often sparse and, in some respects, incorrect as no validation processes will have taken place. There is a risk that member banks may need to split the focus of its resources from containment measures to information gathering to enable reporting. This would be to the detriment of impacted customers and other affected stakeholders. Some member banks therefore propose that we remain at two timelines for reporting i.e. • immediate notification (within 24 hours) with a description of the event and all information which is known at the time. However, the banks support a recommendation to change this to 48 hours. This will allow the technical teams to focus on response and containment measures without diverting attention to reporting requirements in the first 24 hours of an incident. The extended time will also allow time for more deliberate internal review and governance processes for ensuring accuracy of the materiality rating and obtaining governance approvals to ensure only known and validated content is being reported.	Disagree. The Authorities are of the view that the current reporting requirements are sufficient. See response to comment 69 above. It must be noted that early visibility on incidents is critical for timely regulatory engagement.

				- a 14-day subsequent update(s) to remain unchanged – as per annexure A; and - it should be included in the directive that the banks should report all known and validated information at the time the reports are due, acknowledging that it is likely that some information may not be known at the time.	
79.	BASA	Cover page	11; B	The current wording appears to be incomplete and should refer to Joint Standard 1 of 2023 at the end of the sentence.	Noted. The cover page was updated to “Within 24 hours following the discovery of a material incident as per the Information Technology Governance and Risk Management Requirements - Joint Standard 1 of 2023”.
80.	BASA	Cover page	12; B	The current wording appears to be incomplete and should refer to Joint Standard 2 of 2024 at the end of the sentence.	Noted. The cover page was updated to “Within 24 hours following the discovery of a material incident as per the Cybersecurity and Cyber Resilience - Joint Standard 2 of 2024”.
81.	BASA	Cover page	14; C	The requirement to submit a final investigation report is noted and clarity is requested on whether there are any specific requirements for this report. It is preferred that each institution can submit their current investigation reports as all required information is contained therein.	Noted. There are no specific requirements for this report, each institution can submit their final investigation report.
82.	BASA	Details of the incident	8; A	1. The intention of this question is not clear. Is it intended to determine if any other regulators were notified of the incident or if this report form was sent to other regulators? We suggest the following wording to ensure clarity. ‘Has any other regulatory authority (e.g. NPSD, Information Regulator) been notified of this incident?’ Regulators are generally notified simultaneously therefore an attachment would not be available or could well be the report form proposed by the joint determination. It is requested that institutions are able to select the authorities to which they have reported the incident via tick boxes.	Noted. The template has been updated to “Has any other regulatory authority (e.g. NPSD, Information Regulator) been notified of this incident”. The question is now row 18. ‘Attach notification(s)’ to be replaced by “provide more details”.

83.	BASA	Details of the incident	8; A – 18; A	The regulator is requested to reconsider the current flow of questions and amend as follows: move A8 down and start with A9, A15, A14. This will allow for a logical flow starting with the incident and then moving on to materiality and notifications.	Noted, the Authorities have updated accordingly.
84.	BASA	Details of the incident	8; B	If the PA/FSCA is the first authority to be informed, e.g. it sometimes takes longer than 24 hours to detect if an incident resulted in the loss of PI data for reporting to the Info. Regulator, a Yes/No option may not be appropriate. Consider adding a “To be determined” or similar option.	Noted. The reporting template has been amended to “to be determined”.
85.	BASA	Details of incident	10; B	We have numerous criteria which we consider when rating an incident as material. Many of these criteria may not have influenced the rating and will have been omitted in the assessment. We should only be required to include the criteria from our list that influenced the outcome of the rating.	Noted, given that this is a free text question, institutions are encouraged to provide as much detail on the criteria used to determine the rating.
86.	BASA	Details of the incident	12; A	The following information may not be available within 24 hours: “Business lines affected”. We recommend moving it / completing it as part of the Incident details that will be completed as a subsequent update.	Noted, it is important throughout the process as section A provide high level of the business based on initial assessment, then section B and C is based on additional and the final assessment. Please note that this information is reporting 24 hours after the incident is categorised as material and not 24 hours after the incident.
87.	BASA	Details of the incident	12,14; A	This information may not be available within 24 hours and therefore we would appreciate an allowance to submit all known details on the material incident form within 24 hours and for the remaining information to be submitted within the 14-day timeline.	See response to comment 24 and 86 above.
88.	BASA	Cyber incident info	11 - 16; B	It is our view that the following questions will require more time to ascertain and request that these questions be moved to the “impact of the incident” tab due within 14 calendar days: Cause of incident: Category of attackers: Type of attack (e.g., DDoS, Ransomware etc) What vulnerabilities/weaknesses were exploited?	Disagree. The Authorities are of the view that this must be completed on a best-efforts perspective and can be updated at a later stage.

89.	BASA	Cyber incident info	11; A	1. Please explain further what you mean by origin. 2. If intended to focus on origin of incident detection, then is it whether the institution detected it through internal monitoring? Alternatively, is it intended to focus on the origin of incident itself, i.e. whether it is caused by an external threat actor?	Noted. The template has been amended by changing 'Origin' to "Origin of the threat". The question is now row 12.
90.	BASA	Cyber incident info	12 - 13, 16; A	This information may not be available within 24 hours and therefore we would appreciate an allowance to submit all known details on the material incident form within 24 hours and for the remaining information to be submitted within the 14-day timeline.	See response to comment 86 and 87 above.
91.	BASA	Cyber incident info	13; A	Category of Attackers is quite subjective and sometimes, it might apply to one or more categories. We suggest multiple answer selection option should be considered.	Noted. There is provision for free text on column C which should cater for additional information (i.e. multiple answers).
92.	BASA	Cyber incident info	13; B	Reconsider the term 'script kiddie' in the drop-down. Consider using a more formal term like: 'low-sophistication attacker, unskilled threat actor, opportunistic attacker'...etc.	Noted. The term 'script-kiddies' is a widely used cybersecurity term, however term has be augmented to read to "Script-kiddies (novice attacker)". The question is now 14.
93.	BASA	Cyber incident info	14; A	BASA recommends that 'type of attack' be a dropdown with a predefined list of attack types. Different organisations may have a different understanding of incident classification and attribution, and this may lead to inconsistencies.	See response to comment 60 above.
94.	BASA	Cyber incident info	16; A	It is requested that the regulator include a structured list of vulnerabilities and control weaknesses, aligned to NIST or ISO standards. This should allow for multi-select and an "Other" option, plus referencing supporting evidence like CVEs or scan IDs. The current version includes a drop down with 12 options, e.g. inadequate user access management among others.	Noted. Vulnerabilities, however, are continuously evolving, the template may thus require continuous updating to keep up with the changes. The version circulated for consultation does not have the dropdown list, but free text.
95.	BASA	Cyber incident info	16; B	Financial institutions should not be required to provide direct information regarding the specific vulnerabilities or weaknesses exploited in an incident report. The incident itself is adequately described in the 'Details of the Incident' and 'Impact of the Incident' sections, and further disclosure of vulnerabilities is unnecessary. Information about vulnerabilities and weaknesses is highly sensitive; sharing it with	All information provided to the Authorities will remain confidential and may only be disclosed in accordance with sections 250 and 251 of the FSR Act. It is essential that the regulator is aware of the vulnerability, as this risk directly threatens both customer protection and the

				regulatory bodies, especially without clear understanding of their security practices or who will access the reports, poses a significant security risk. Therefore, financial institutions will not provide this information and will leave this reporting field blank. We strongly recommend that this data field be removed from the template. Notably, similar fields have been excluded from other incident reporting regimes, such as the EU Digital Operational Resilience Act, and SARB should adopt a similar approach.	financial stability of financial institutions core responsibilities of the Authorities.
96.	BASA	Cyber incident info	General	It is requested that a free-form text field is included for the institution to indicate how the incident was discovered.	Noted. A free-form text field has been added to the template.
97.	BASA	Impact of the incident	9; A	It is not clear what an unauthorised release of data would mean in this instance. If the intention is to elicit whether the attackers subsequently published the information to the public or on the dark web we propose the following wording: <i>"Following the incident, was any of the compromised information subsequently published either publicly or on the dark web?"</i> If the intention is to elicit whether the attack itself resulted in the exposure of data to the attacker, we propose that the wording used in the Protection of Personal Information Act, 2013 be used as follows: "Has an unauthorised access or unauthorised acquisition of data occurred?" If a person accidentally shared data to a person that it was not meant to be shared with – is this classified as unauthorised release of data?	See response to comment 56 above.
98.	BASA	Impact of the incident	9 -11; A	Information regarding data sensitivity is proprietary and inherently sensitive to both financial institutions and their customers. Accordingly, data fields 9, 10, and 11 should not require detailed information about the sensitivity or compromise of data. The business and customer impact of incidents is already addressed in other fields and could be consolidated into a single field concerning the materiality of the incident for customers. Financial institutions are committed to protecting customer data and are unlikely to provide detailed information in these fields. We recommend these fields be deleted.	See response to comment 95 above.
99.	BASA	Impact of the incident	9 - 53; A	The data fields required by SARB are overly prescriptive and detailed, often including information not directly related to the incident or split across multiple fields. The Financial Stability Board (FSB) has	The Authorities have considered the FSB's (FIRE) template; however the template emanates from two Joint Standards (Cyber

				developed the Format for Incident Reporting Exchange (FIRE) template, which we encourage SARB to align with. The SARB template is unnecessarily complex and could substantially reduce the number of required fields. For example, the 'Impact of Incident' section includes 22 fields, whereas FIRE proposes only 8; similarly, SARB proposes 21 fields for resolution, while FIRE suggests 12. We further recommend the inclusion of 'optional' or 'essential' designations for data fields. For instance, if an incident does not impact customers, the corresponding field should not be mandatory. The FSB template is designed for international harmonisation among financial regulators, and we encourage SARB to adopt it to reduce reporting burdens and fulfil the FSB's mandate.	and IT) and incorporate requirements from both prudential and conduct perspectives.
100.	BASA	Impact of the incident	10; A	Grammar – Other rows ask a question; this one is a statement. Consider writing it out as “ “Was sensitive customer data leaked?” Sensitive customer data is not a definition that is found in the joint standards, can this be defined?	Noted. The template has been amended to read: “Was sensitive customer data leaked?” The question is now row 11. Sensitive customer data must be interpreted as 'sensitive information' which is defined in the Joint Standard 2 of 2024 - Cybersecurity and Cyber Resilience. See response to comment 20 above.
101.	BASA	Impact of the incident	12; A	1. It is requested that the question is amended to the following: Are there measures in place to assess the potential impact of the incident on customers?' Responses limited to 'Yes' or 'No' to avoid unnecessarily lengthy responses. 2. Assessing incident impact is generally well established and integrated into the institution's incident management process. The FSCA is requested to clarify their regulatory expectations to ensure certainty in application. This will be a standard response based on materiality/severity/Cyber Crisis Management Team and will not shift between responses.	Noted. To understand the scope and extent of the measures each financial institution implemented (relating to the assessment of the potential impact of the incident on customers) is a key supervisory priority. This supports the application of proportionality and facilitates effective supervision which embraces taking into account the unique risk profile of the client.

102.	BASA	Impact of the incident	13; B	Number of customers should be populated in free text however the response field includes a drop down which must be removed.	Noted. The template has been amended accordingly.
103.	BASA	Impact of the incident	14; B	Tick boxes with potential stakeholders are preferred to ensure completeness. User will only select the applicable stakeholders.	Disagree. Financial institutions may have different stakeholders. Financial institutions may include potential stakeholders to go beyond the provided options.
104.	BASA	Impact of the incident	16; A	Claims related to operational, or ICT incidents may arise months or years after incident resolution. If a claim is made, there is often a significant delay before any determination is reached. Financial institutions are unlikely to provide information about individual customer claims, as this is sensitive and may be subject to legal dispute. Requiring this data field at the time of resolution is therefore of limited value, as claims are unlikely to have been made within the reporting timeframe. We recommend this field be removed due to the lack of available information and the inability to provide details about the claims process. It is also not clear if this is customer claims or insurance claims.	Noted. The template has been amended to read "have any claims been lodged against the financial institution as a result of the incident. The question is now row 17 Institutions are required to provide details based on available information.
105.	BASA	Impact of the incident	17 - 21; A	Data fields concerning customer communication, rights information, support services, enhanced customer service, and service continuity are not directly related to the operational incident, its business impact, or resolution. We recommend that SARB not use the incident reporting template to mandate financial institution actions, but rather to gather information about the incident and its resolution. SARB already has regulations and supervisory capabilities regarding consumer policy. Incident reporting templates are not the appropriate mechanism for enforcing consumer policy outcomes. We recommend these fields be removed, as they are unrelated to incident remediation or impact. Any consumer policy information can be provided through supervisory channels, not incident reporting.	From the FSCA's mandate perspective, we need to assess impact on customers to ensure market conduct and fair customer outcomes. While it may not seem as a mechanism for consumer policy, incidents are utilised as a trigger for supervisory action. Operational incidents cannot be viewed in isolation from conduct risk implication, consequently, inclusion of data regarding customer communication and service continuity is a necessary mechanism that would assist supervisors.

106.	BASA	Impact of the incident	18 - 19, 21 - 22; A	1. It is requested that customer impact is determined at the onset, and should the response be 'no', the rest of the customer-related questions are marked as not applicable. 2. It is important for the regulators to consider the responses to all questions and their expectations in terms of the value derived from these responses. It is recommended that certain questions can be combined and/or rephrased to garner more valuable responses.	1. Noted. Should the response be 'no', the financial institution can mark the rest of the customer-related questions as 'not applicable'. 2. Disagree with the proposal to combine the certain questions, as the current granular fields are designed to accommodate various operational and conduct metrics. Merging the fields risks creating vague and obscure data points, and may frustrate the objective assessment of materiality by the Authorities.
107.	BASA	Impact of the incident	18 - 19; B	It is important for the regulators to consider the responses to all questions and their expectations in terms of the value derived from these responses. It is recommended that certain questions can be combined and/or rephrased to garner more valuable responses. This will be a standard response based on materiality/severity/Cyber Crisis Management Team and will not shift between responses.	Noted. See response to comment 106 above.
108.	BASA	Impact of the incident	19; A	"Are there any provisions in place for enhanced customer service?" We request clarification of the intention of this question, considering the customer focused question preceding it.	See response to comment 105 above.
109.	BASA	Impact of the incident	22; A	1. The response to this question would be very complex and would require engagements across all institutions involved. It is recommended that this is excluded from the report form as it will be provided in the final investigation report. 2. It is important for the regulators to consider the responses to all questions and their expectations in terms of the value derived from these responses. It is recommended that certain questions can be combined and/or rephrased to garner more valuable responses.	Disagree. Each financial institution must have a view of their current controls to mitigate specific threats in the environment.
110.	BASA	Impact of the incident	29; A	Financial institutions are unlikely to provide detailed information regarding whether an incident constituted a breach of legal or regulatory requirements. Such information carries significant legal implications and is highly sensitive, making it inappropriate for inclusion in incident reports to the regulator. This data field was removed from the EU Digital	1. See response to comment 95 above. 2. Disagree, the Authorities are of the view that the wording is sufficient to capture responses at a particular point. Financial institutions can

				Operational Resilience Act, recognising the legal risks involved. We recommend SARB amend this field, as financial institutions are unlikely to provide detailed responses or confirmations of breaches. Additionally, member banks are of the view that this question is too broad and out of sync with other similar legislative provisions. We suggest the following amendment: "Was there any material breach of legislative obligations?"	update their responses as more information becomes available about the nature and materiality of the breach.
111.	BASA	Impact of the Incident	29; A	For global SA firms, is the scope of this question limited to SA or also applicable to international jurisdictions? Suggest this is clarified.	The Joint Standard applies to financial institutions that are licensed in the Republic. It is advised, however, that some incidents make originate at a -parent company/branch/subsidiary/associate located outside the Republic but may have repercussions to the parent company/branch subsidiary in the Republic.
112.	BASA	Impact of the incident	29; B	The response in column B could be a drop-down (yes/no), followed by details if yes.	Noted. The template has been amended accordingly.
113.	BASA	Impact of the incident	30; A	Media coverage may on occasions not be immediate. We have seen media engagement on issues up to 8 months after the incident. How will the reporting account for that scenario?	See response to comment 63 above.
114.	BASA	Impact of the incident	33; A	The entry vector for a cybersecurity breach is highly sensitive, and sharing this information in an incident report constitutes a significant security risk. Financial institutions will not provide this information, and we recommend this data field be deleted.	See response to comment 95 above.
115.	BASA	Impact of the incident	34; A	What is meant by "factors". I see this is free text. Could this please be more specific, or a drop down?	The template has been amended to read "what caused the incident to occur?". The cause of the incident may be different for each incident; thus, a prepopulated dropdown is not feasible. The question is now row 35.
116.	BASA	Impact of the incident	35; A	Please clarify the nature and form of "incident response plan"? Will this include the likes of a crisis management team, or does it relate to the Cyber Security Incident Response Team (CSIRT)?	Incident response plan processes differ from financial institution to financial institution based on the incident; thus the Authorities will

				Seems unnecessary to indicate that an incident response plan has been activated. Reporting a material incident would imply that an incident response plan was activated.	not prescribe the form and nature of the incident response activation. See response to comment 65.
117.	BASA	Impact of the incident	43; A	Consider changing the term 'police' to 'law enforcement'.	See response to comment 48.
118.	BASA	Impact of the incident	45; A	The reference to 'channels of communication' needs to be clarified to ensure the correct response is obtained i.e. who is the intended target audience of communication? Would it be all stakeholders or those involved in the investigation such as the Police?	Noted. Question 42,44, 45 has been removed. The Authorities do not prescribe the communication channels to stakeholders. The form and manner in which the financial institution conducts usual escalations will suffice.
119.	BASA	Impact of the incident	46, 53; A	Financial institutions are unlikely to have determined their long-term strategies or future training sessions for operational incidents immediately following an incident, especially before its resolution. Some incidents may not necessitate changes in long-term strategies or training and may be unique, not reflecting broader security practices. Long-term security practices and strategies are better addressed through supervisory engagement with the regulator, not incident reports. We recommend SARB remove these data fields, as they are unlikely to yield useful information.	Disagree. The question has, however, been amended to read "What strategies will be implemented to prevent recurrence of such incident?" The question is now row 44. Additionally, financial institutions have an opportunity to provide detailed information as per the reporting requirements - see response to comment 24 above. The question "Are there measures in place for future training sessions based on lessons learnt from this incident?" has been removed.
120.	BASA	Impact of the incident	48; A	Indirect financial cost is highly subjective and often does not provide useful information to either the financial institution or the regulator. It is unclear what this cost entails or how it would inform the regulator about the incident's impact and resolution. Data field 47 should be sufficient to determine the cost impact of any incident. We recommend SARB amend this data field.	Noted. The Authorities have removed the ranges and enabled input for free text for 47, 48 and 49. The Authorities are expecting the financial institutions to provide information on a best-efforts basis.
121.	BASA	Impact of the incident	50; A	Guidance is requested on the regulator's expectation with this response. Civil liability and professional indemnity cover may only be finalised sometime after the incident and therefore it requested that the question	It is important to note that professional indemnity cover is important in an event that the incident involves

				is changed to a Yes/No on whether the option of civil liability and/or professional indemnity cover will be pursued. Additionally, this information is not directly relevant to the incident's impact or resolution, and its necessity is unclear. We recommend SARB to consider removing this data field.	customer/investor/member loss, therefore as the Authority we are invested in understanding the availability and extent of professional indemnity cover to ascertain and satisfy ourselves as to whether customers/investors/members will be placed in a position they were before the incident occurred. Further, Authorities need to understand if the financial institution has funds/liquidity to satisfy claims in an event the insurance claim is rejected.
122.	Institute of Retirement Funds Africa NOC	Cover Page	A 11-12	Comment: The meaning of "impact of the incident tab" is unclear. Recommendation: We recommend re-wording or clarifying this phrase to avoid confusion.	Noted. The Authorities have amended the template in column C to provide clarity.
123.	Institute of Retirement Funds Africa NOC	Cover Page	A 11-12	Comment: Some incidents may be discovered outside of standard business hours. It is unclear whether the 24-hour notification period applies to incidents discovered outside of standard business hours (e.g., on weekends or public holidays). Recommendation: We recommend clarifying that the 24-hour notification period should be calculated from the next business day for incidents discovered outside of standard business hours, or alternatively that the notification period be extended to 48 hours.	The 24 hours is after classifying the incident as material, irrespective of whether the incident was discovered outside of business hours. See response to comment 24 above.
124.	Institute of Retirement Funds Africa NOC	Cover Page	A14	Comment: The term "full incident report" is not clearly defined. It is unclear what information should be included beyond the completed notification template. Recommendation: We recommend including a checklist or guidance on what constitutes a "full incident report", including whether it should include external investigation reports, forensic analysis, legal opinions, or other supporting documentation.	Disagree. The Authorities do not prescribe the form and manner of the full incident report which entities submit as they conclude their investigation. This will be dependent on the scope and nature of the incident which will differ from time to time. The template is a basis of the investigation; however, the tailored report will differ from institution to institution.

125.	Institute of Retirement Funds Africa NOC	Contact Details	A8-19	Comment: To ensure accountability and continuity, we recommend making the inclusion of a second contact person mandatory. This would ensure that the Authorities can always reach an accountable individual if the primary contact is unavailable. Recommendation: We recommend that "Person 2" be a mandatory field. Person 2 must be appointed Information Officer or Deputy Information Officer	Disagree. The first contact person is mandatory. Given the size, nature and complexity of our supervised institutions, some institutions may not have an alternative contact person.
126.	Institute of Retirement Funds Africa NOC	Details of the Incident	A9	Comment: Not all financial institutions (e.g., smaller institutions and pension funds) will be capable of detecting incidents in real time. Recommendation: We recommend allowing for "approximate date/time" where exact logs are unavailable.	See response to comment 24 above.
127.	Institute of Retirement Funds Africa NOC	Details of the Incident	A14	Comment: The reference to "customer" does not align with the terminology of the Pension Funds Act and does not appropriately recognise the retirement fund context. Recommendation: We recommend that the term "customer" be replaced with "financial customer" (as defined in the FSR Act) or "member" to align with the legislative framework. This change should be made throughout the template.	Noted. The template has been amended to reference a financial customer under A14. For the purpose of this report, a customer shall be understood to mean a financial customer, and this include members and beneficiaries as defined in the Pension Funds Act.
128.	Institute of Retirement Funds Africa NOC	Details of the Incident	A16	Comment: There is no direction as to what "classification" a preliminary incident may fall into. Recommendation: We recommend adding guidance notes to assist with accurate classification from the dropdown menu.	The Authorities are of the view that the dropdown options are clear The Authorities will consider issuing guidance on the classifications.
129.	Institute of Retirement Funds Africa NOC	Cyber-Incident Info	A10	Comment: Incidents may be discovered by individuals or by IT systems. It is unclear whether this refers to the individual who discovered the incident or the system that discovered the incident. Recommendation: We recommend clarifying whether this refers to the person or the system.	The Authorities are referring to a function. The tools and technologies can detect an incident; however, this will still require a review. The questions have been rephrased to include examples such as Security Personnel, Third-Party, Internal Audit or Other.

130.	Institute of Retirement Funds Africa NOC	Cyber-Incident Info	A11, A12, A13	Comment: There is no direction as to what the "origin", "cause", or "category" of an incident may be. Recommendation: We recommend adding guidance notes to assist with accurate identification from dropdown menus.	See response to comment 40 above. The Authorities are of the view that the dropdown options are clear. The Authorities will consider issue guidance on the classifications.
131.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A9	Comment: It is unclear whether "unauthorised release" includes only external breaches or whether it includes internal misuse. Recommendation: We recommend clarifying whether "unauthorised release" also includes internal misuse or only external breaches.	See response to comment 42 above.
132.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A10	Comment: "Sensitive data" is not a defined term, but "sensitive information" is. It is unclear whether "leaked" refers to internal incidents or only external breaches. Recommendation: We recommend replacing any references to "sensitive data" with "sensitive information" and clarifying whether "leaked" refers to internal incidents or only external breaches.	Sensitive data must be interpreted as sensitive information as defined in Joint Standard 2 of 2024 - Cybersecurity and Cyber Resilience. See response to comment 20 above.
133.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A13	Comment: It may be difficult to ascertain the exact number of customers impacted. For investment or benefit administrators, one institution (e.g., fund) may be affected, but many more underlying retail customers/members may be impacted. Recommendation: We recommend that this field require information on "estimated" total number of financial customers impacted and suggest adding a comment that this should be the number of underlying retail customers/members.	Agree. The Authorities have rephrased the field to read as "Estimated total number of customers impacted". The dropdown was amended to a free text field. The question is now row 14.
134.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A15	Comment: It may be useful to have copies of the communication to stakeholders. Recommendation: We recommend requiring a copy of communication and the date the communication was made. We also suggest adding a row asking WHEN stakeholders were informed.	Disagree. The Authorities do not prescribe the form and manner of communication to stakeholders. The form and manner in which the institution chooses to utilise in order to communicate will suffice.

135.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A16	Comment: Some claims may have arisen or been instituted before the financial institution has knowledge. There is also no direction as to what "classification" a preliminary incident may fall into Recommendation: We recommend adding the words "that you are aware of" between the words "arise" and "due" and adding guidance notes to assist with accurate classification from drop down menu	Noted. This has been reworded to "Have any claims been lodged against the financial institution as a result of the incident". The question is now row 17. As for the preliminary classification of the incident, the Authorities are of the view that the dropdown options are clear.
136.	Institute of Retirement Funds Africa NOC	Impact of the Incident Impact of the Incident	A20	Comment: The meaning of "enhanced customer service" is not clear. Recommendation: We recommend rewording the question as follows: "As a result of the incident, are there any provisions in place for enhanced customer service?" and suggest adding examples from a dropdown menu.	Enhanced customer support is not similar to the standard service offering with standard SLA, enhanced customer support requires faster SLAs, dedicated response team, priority, pro-active and responsive.
137.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A28	Comment: It would be useful to know the role of the third-party service provider in the financial institution. Recommendation: We recommend including what the third-party service provider's role is.	Disagree. The question must be read in conjunction with question 24 and 25 for context. All responsibilities for compliance with the Joint Standards rest with the financial institution.
138.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A29	Comment: It would be useful to have a list of legal or regulatory requirements breached. Recommendation: We recommend requiring a list of legal or regulatory requirements breached. Also correct typo: "Was there any breach of legal or regulatory requirements?" (plural).	Disagree. Although the template inquiries about breach of legal or regulatory requirements, financial institutions are expected to comply with relevant sectoral laws. The template was amended to read "Was there any breach of legal or regulatory requirements?" The question is now row 30.
139.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A30	Comment: It would be useful to have a link to the media coverage if available. Recommendation: We recommend requiring a link to the media coverage if available.	Disagree. The Authorities are of the view that providing a link to the media coverage is not necessary at this point in time.

140.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A33	Comment: The term "entry vector" is esoteric and may not be understood by non-technical staff or boards of trustees. Recommendation: We recommend adding an explanation of what "entry vector" means or using more accessible terminology.	Disagree. The Authorities are of the view that the information will be sourced from technical individuals, however, the Authorities may consider a comprehensive guideline in future.
141.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A35, A36, A37	Comment: Consistency in capitalisation is needed. Recommendation: We recommend capitalising as follows: "Was the Incident Response Plan activated?", "Was the Disaster Recovery Plan (DRP) activated?", "Was the Business Continuity Plan (BCP) activated?"	Noted. The template has been updated accordingly.
142.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A38	Comment: It may be useful to have evidence that the incident was reported to the Board. Recommendation: We recommend that the Board must endorse all reporting by the administrator.	Noted. The Authorities are of the view that it is not necessary to attach evidence at this point, however, the Authorities may require this on a case-by-case basis.
143.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A42	Comment: It may be useful to have further details of the lead of the investigation. Recommendation: We recommend including the lead investigator's designation and contact details.	Question 42 has been removed from the template.
144.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A47, A48, A49	Comment: It may be difficult for pension funds to quantify the financial loss of an incident in rand terms, as the impact is often operational (e.g., delayed processing of benefit payments, inability to update member records). For insurers or administrators, it would be easier to quantify loss. Requiring immediate financial quantification may lead to speculative or inaccurate estimates. Recommendation: We recommend allowing for a narrative description of the loss, in addition to or instead of a rand value. Specifically: (A47) "Estimate direct financial loss in Rands, or provide a qualitative description of operational impact"; (A48) "Estimate indirect financial loss in Rands, or provide a qualitative description of reputational or other non-financial impact"; (A49) "Estimation of the financial impact on	Noted. See response to comment 50 above. The Authorities expect the financial institutions to provide information on a best-efforts basis. Disagree. The rand values are still required; however financial institutions have an opportunity to provide additional information on column C.

				financial customers in Rands, if available, or provide a qualitative description of service disruption or member inconvenience". Also add the words "if information is available" after the word "Rands".	
145.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A50	Comment: Proceedings for recovery may not have been concluded by the time the report is submitted. Recommendation: We recommend that this be reworded to make provision for potential recovery as well.	Noted. See response to comment 24 above. Financial institutions can amend the notification as new information is sourced.
146.	Institute of Retirement Funds Africa NOC	Impact of the Incident	A53	Comment: The requirement for pension funds and administrators to submit notifications via email raises concerns about security, tracking, and potential for technical failures (e.g., emails being delayed, lost, or blocked by spam filters). There is no automated acknowledgment of receipt or audit trail. Recommendation: We recommend that the Authorities provide an alternative, secure submission mechanism, such as a dedicated portal, for all financial institutions. If email submission is retained, the Authorities should implement automated acknowledgment of receipt and provide clear guidance on encryption and security requirements.	Please note that the FSCA has resolved to establish a dedicated submission portal, namely the Joint Standards Submission Portal, which is scheduled to be effective/operational on 01 September 2026. With regards to "acknowledge of receipt", it is envisaged that the portal will have a report / audit trail capability. In addition, the portal will upon submission by the regulated entity issue automated "notification / acknowledge of receipt". Please see response to comment 22 above as well.
147.	Institute of Retirement Funds Africa NOC	General	All sheets	Comment: The template requires highly technical information but does not provide definitions or examples for many technical terms. Recommendation: We recommend that the Authorities publish comprehensive guidance notes to accompany the template, including definitions of technical terms, examples of incident classifications, and illustrative scenarios. This guidance should be developed in consultation with industry participants to ensure it is practical and fit for purpose.	The Authorities are of the view that the information will be sourced from technical individuals, however, the Authorities may consider a comprehensive guideline in future.

148.	ITLawCo	Details of the Incident	General	Mark which fields are mandatory in the 24-hour initial notice versus those that can be updated in the 14-day or final report. This avoids unrealistic expectations of complete RCA within 24h.	Noted. However, see response to comment 24 above.
149.	ITLawCo	Cyber Incident Info	Drop-down categories (Options sheet)	Drop-down list is comprehensive but may lag behind emerging threats (e.g., supply chain attacks, AI-driven exploits). We recommend FSCA commit to annual updates of the taxonomy.	See response to comment 60 above.
150.	ITLawCo	Impact of the Incident	Root cause and impact analysis	Complex RCAs cannot always be finalised in 14 days. Recommend FSCA permit interim assessments, with full RCA required in the final report.	See response to comment 24 above. The Authorities are of the view that the reporting in stages provides ample time for financial institutions to comply.
151.	ITLawCo	Options Sheet	Affected Areas	Current list includes ATMs, core banking, payments. Recommend adding cloud infrastructure, APIs, and mobile channels, reflecting modern financial dependencies.	Noted. The Authorities acknowledge that the template may require periodic updating. Thus, the Authorities have collapsed the drop-down where appropriate and have provided the option of selecting 'Other' and provided a free-text field for clarification.