GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$18.00 WINDHOEK - 19 June 2026 No. 8954

CONTENTS

Page

General Notice

BANK OF NAMIBIA

No. 422 2026

DETERMINATION ON INFORMATION SECURITY:
BANKING INSTITUTIONS ACT, 2023 (ACT NO. 13 OF 2023)

In my capacity as Governor of the Bank of Namibia, and under the powers vested in the Bank in terms of section 108(3)(b) of the Banking Institutions Act, 2023 (Act No. 13 of 2023), I hereby issue the Determination on Information Security (BID-30*)*.

EBSON UANGUTA
GOVERNOR

DETERMINATION NO. BID-30

DETERMINATION ON INFORMATION SECURITY (BID-30)

ARRANGEMENT OF PARAGRAPHS

PART I
PRELIMINAY PROVISIONS

1. Short Title – Determination on Information Security.

2. Authorisation – Authority for the Bank to issue this Determination is provided in section 108(3)(b) of the Banking Institutions Act, 2023 (Act No. 13 of 2023).

3. Definitions – Terms used within this Determination are as defined in the Act, as defined below or as reasonably implied by contextual usage:

3.1 "Availability" means timely and reliable access to and use of information;

3.2 "Bank" means the Bank of Namibia as defined in the Bank of Namibia Act, 2020 (Act No. 1 of 2020);

3.3 "Banking institution" means as defined in the Act a public company authorised under the Act to conduct banking business as defined in the Act;

3.4 "Common Equity Tier 1 capital" means as defined in the Determination on the Measurement and Calculation of Capital Charges for Credit Risk, Operational Risk and Market Risk for Domestic Systemically Important Banks (BID-5A);

3.5 "Confidentiality" means ensuring that sensitive information, including private and proprietary information, is not accessed or disclosed to unauthorised individuals, entities, processes or systems;

3.6 "Cyberattack" means the use of an exploit by an adversary to take advantage of weaknesses with the intention of achieving an adverse effect on the Information Communication and Technology environment of a banking institution or a microfinance banking institution;

3.7 "Cyber governance" means arrangements that a banking institution or microfinance banking institution puts in place to establish, implement and review its approach to managing cyber risk;

3.8 "Cyber incident response plan" means the documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber incident;

3.9 "Cyber risk" means the combination of the probability of an event occurring and the consequences of that event;

3.10 "Cyber risk management" means the process used by a banking institution or a microfinance banking institution to establish an enterprise-wide framework to manage the likelihood of a cyberattack and develop strategies to mitigate, respond to, learn from and coordinate its response to the impact of a cyberattack;

3.11 "Cybersecurity" means the protection of information systems, including hardware, software, networks, and data from cyber threats in order to maintain confidentiality, integrity and availability;

3.12 "Data at rest" means data that has reached a destination, stored and is not being accessed or used;

3.13 "Data in transit or motion" means data that is actively moving across devices and networks;

3.14 "Data in use" means data actively being used across networks or temporarily residing in memory, or any data not in use or classified as inactive;

3.15 "Framework" means the policies, procedures and controls established to identify, protect, detect, respond to, and recover from information security incident risks, including cyber risk. A banking institution or microfinance banking institution may adopt any appropriate designation for its framework, provided it meets the requirements of this Determination;

3.16 "Information" means data in any form that is processed, organised, or structured so as to have meaning, including when printed, written, stored electronically, transmitted, or communicated verbally;

3.17 "Information security" means the preservation of the confidentiality, integrity and availability of information, and includes cyber security;

3.18 "Information security event" means any observable occurrence indicating a possible breach of information security or failure of controls;

3.19 "Information security incident" means any single or series of information security events that compromise the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, and includes cyber incident;

3.20 "Integrity" means the completeness, accuracy and reliability of data, information systems or any part thereof, including the protection against unauthorised modification or destruction;

3.21 "Malicious programs" means programs such as viruses, worms, Trojan horses, ransomware, spyware, adware, shareware, and any other method, designed to spread and replicate from one computer to another through communications links, or through the sharing of electronic files, to interfere with or damage computer operation, and malware has the same meaning;

3.22 "Microfinance banking institution" means as defined in the Act;

3.23 "Need to know basis" means to limit access to sensitive information only to those whose official duties requires it.

3.24 "Outsourcing arrangement" means a written, legally binding agreement between a banking institution or a microfinance banking institution and a service provider, by which a service provider performs a business activity, function or process which can ordinarily be undertaken by the banking institution or a microfinance banking institution itself;

3.25 "Penetration testing" means the practice of testing a computer system, network or web application for security weaknesses or vulnerabilities that might potentially be exploited;

3.26 "Recovery point objective" means maximum acceptable level of data loss following an unplanned event, also referred to as maximum acceptable data Loss;

3.27 "Recovery time objective" means the period following an incident within which a product or an activity or resources must be recovered;

3.28 "Resilience" means the ability to anticipate, withstand, detect, respond to and recover from an incident, while upholding confidentiality, integrity and continuity of the institution's critical operations. In this Determination, this term is also referred to as "cyber resilience";

3.29 "Respond" means the development and implementation of appropriate activities and capabilities by a banking institution or microfinance banking institution to take immediate action when a cyber event is detected;

3.30 "Risk tolerance" means the level of risk a banking institution or a microfinance banking institution is willing to assume to achieve a potential desired result. For the purpose of this Determination, this term is also referred to as "cyber risk tolerance";

3.31 "Situational awareness" means the ability of a banking institution or microfinance banking institution to identify, process and comprehend the critical elements of information through

a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event;

3.32 "Strategy" means a banking institution or a microfinance banking institution's high-level principles and medium-term plans for managing cyber risk. A banking institution or microfinance banking institution may refer to this Strategy using a relevant naming convention, such as Information Security Strategy, Cyber Resilience Strategy or any other equivalent term aligned with the banking institution or a microfinance banking institution's risk management framework;

3.33 "Threat" means a circumstance with the potential to exploit one or more vulnerabilities that adversely affects the security of an institution. In this Determination, this term is also referred to as "cyber threat";

3.34 "Threat intelligence" means threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes;

3.35 "Vulnerabilities**"** means weaknesses or flaws in information systems, applications, networks, processes, or controls that could be exploited by a threat to compromise the confidentiality, integrity or availability of information or systems;

3.36 "Vulnerability assessments" means a process of identifying, quantifying, and prioritising or ranking the vulnerabilities in a system; and

3.37 "Zero trust" means a security model that assumes no user, device, or system is inherently trustworthy. Access to resources is strictly limited and continuously verified based on identity, context, and risk level, regardless from where the request originates.

PART II
STATEMENT OF POLICY

4. **Purpose** – This Determination establishes key principles on measures to protect banking institutions and microfinance banking institutions against current and emerging information security threats. The Determination aims to ensure operational resilience and reduce the overall impact on business operations as a result of information security vulnerabilities or information security incidents.

5. **Scope and Application** – This Determination applies to all banking institutions and microfinance banking institutions authorised by the Bank to conduct banking business and microfinance banking business in Namibia. It covers all information assets, systems and processes, whether managed internally or through third parties, including cloud services, artificial intelligence-driven technologies and interconnected ecosystems. The principles set out in this Determination must be implemented in a manner that reflects the nature, size, complexity and risk profile of the banking institution or microfinance banking institution. Where terms such as appropriate, adequate, effective, timely, regular, or periodic are used, implementation must be assessed in the same context.

6. **Responsibility** – The board of directors of a banking institution or microfinance banking institution must ensure that its information security strategy and framework are aligned with its overall enterprise risk management framewoek.

PART III
IMPLEMENTATION AND SPECIFIC REQUIREMENTS

7. GOVERNANCE

7.1 Role of the Board

(a) The Board of a banking institution or microfinance banking institution must establish and maintain effective governance over a banking institution or microfinance banking institution's information and cybersecurity frameworks.

(b) The Board must ensure integration of early warning indicators into risk management frameworks to facilitate timely identification and response to an incident or incidents.

(c) The Board must ensure integration of effective governance into the broader risk management and operational resilience strategies of a banking institution or a microfinance banking institution.

(d) The Board must approve the banking institution or microfinance banking institution's risk tolerance levels with respect to information and cybersecurity risks.

(e) The Board must ensure that cyber and information security considerations are embedded in strategic decision-making, including digital transformation, outsourcing and the development of new products and services.

(f) The Board must oversee the banking institution or microfinance banking institution's compliance with all applicable laws, regulations, supervisory expectations, and ensure that regulatory disclosures related to information security are accurate and complete.

(g) The Board must ensure that responsibility for information and cyber security governance is assigned to a role that is functionally independent from information technology operations. Such independence must be ensured through direct reporting access to the Board or to a designated sub-committee of the Board.

(h) The Board must ensure that executive management allocates sufficient resources, including financial, technological and human resources, to manage cyber and information security risks effectively.

(i) The Board must set a strong risk culture that recognises the importance of cyber and information security across the banking institution or the microfinance banking institution.

(j) The Board must ensure that information security risks, including cybersecurity risks, are appropriately integrated into the banking institution or microfinance banking institution's risk-based internal audit plan and subjected to periodic independent assurance, proportionate to the institution's risk profile and complexity, to determine the adequacy and effectiveness of the associated controls.

(k) The Board must ensure it possesses, or has access to, sufficient information technology and cyber expertise to understand the banking institution's information security and cyber risk landscape.

(m) The Board must undertake training on cyber risk developments, threat landscapes and emerging technologies at least annually and more frequently where necessary, to maintain effective oversight on information security and cybersecurity matters.

7.2 Executive Management Responsibilities

(a) Executive management must develop, implement and maintain a comprehensive framework. The framework must be aligned with the banking institution or microfinance banking institution's strategy and must be approved by the Board or a Board-appointed committee.

(b) Executive management must implement processes for ongoing identification, assessment, and monitoring of information and cyber risks, including emerging threats, third-party risks, and technology dependencies.

(c) Executive management must ensure that cyber and information risks are recorded and maintained as part of the enterprise-wide risk register or an equivalent institution-wide risk register.

(d) Executive management must implement a formal security awareness program as part of its framework, to make all employees and relevant external parties aware of the applicable information and cybersecurity requirements.

(e) Executive management must appraise the Board, at least four times a year, on the banking institution or microfinance banking institution's information security risk profile to ensure that it remains consistent with the banking institution or microfinance banking institution's risk tolerance as well as the banking institution or microfinance banking institution's overall business objectives.

(f) Executive management must closely oversee the implementation of the banking institution or microfinance banking institution's strategy, framework, policy, procedures and controls by assigning clear responsibilities, monitoring implementation progress and addressing any gaps in a timely manner.

(g) Executive management must establish and regularly test incident detection, response and recovery plans.

(h) Executive management must document all suspected and actual material information and cyber incidents and provide a preliminary report to the Bank within 24 hours, followed by a detailed post-incident analysis outlining response and remediation measures as per the guidance provided in Part IV of this Determination.

7.3 Information Security Framework and Policy

7.3.1 A banking institution or microfinance banking institution must have in place a comprehensive information security framework that meets the following key requirements.

(a) The framework must clearly articulate how the banking institution or microfinance banking institution plan to effectively identify information security risks, determine its information security objectives and risk tolerance.

(b) The framework should be consistent with a banking institution or microfinance banking institution's enterprise risk management framework or a similar framework which addresses enterprise-wide risk.

(c) The framework must, at a minimum, include components relating to governance, identification, protection, detection, response and recovery as contemplated in this Determination.

(d) A banking institution or a microfinance banking institution must extend application of its information security framework to third parties that it enters into material outsourcing arrangements with and ensure that information security controls are considered and enforced by third parties. The materiality of the outsourcing arrangement must be in accordance with the applicable regulatory guidance governing Outsourcing. The banking institution or microfinance banking institution must require these third parties to implement and uphold information security controls that are commensurate with the institution's risk profile and information security standards, to prevent weaknesses that could compromise the institution's information systems or other interconnected systems and services.

(e) The framework must be reviewed at least once every three years, or after a significant change, including changes to systems, processes, organisational structure, or the threat environment, to ensure that it remains relevant.

7.4 Risk Culture and Awareness

(a) The board and executive management of a banking institution or microfinance banking institution must promote a strong information security culture that recognises that staff at all levels have important responsibilities in ensuring information security, cyber resilience and ethical corporate culture. This culture should be conveyed through clear and effective internal communication and should include sharing relevant information about the strategy and framework with all staff.

(b) A banking institution or a microfinance banking institution should develop and promote an appropriate level of awareness and commitment to information security and cyber resilience business-wide, to make all employees and relevant external parties aware of the information security framework or policy, their contribution and responsibility towards the effectiveness of the information security program and the implications of non-compliance.

(c) A banking institution or a microfinance banking institution must continuously create information and cyber resilience awareness and offer training for staff at all levels, including the board and executive management, in line with recognised industry standards for information and cybersecurity and the risk profile of the banking institution or microfinance banking institution. The awareness training must include current information and cyber threats and attack tactics, and relevant appropriate responses to stay abreast of evolving threats and to aid in business-wide situational awareness.

8. IDENTIFICATION AND MANAGEMENT OF INFORMATION ASSETS

8.1. A banking institution or a microfinance banking institution must maintain a comprehensive understanding of its information technology environment by identifying, classifying and managing information assets based on criticality and dependencies, including those managed by third-party service providers.

8.2. A banking institution or a microfinance banking institution must establish and maintain visibility and control over access to critical systems and data, proportionate to its risk environment.

8.3 A banking institution or a microfinance banking institution must ensure that identification and classification of information assets are integrated with other relevant policies and processes, including acquisition and change management, in order to ensure inventories are kept up-to-date, as well as remaining both accurate and complete. Asset management must support risk assessment and protection strategies to ensure visibility and control over all information assets.

8.4. Physical and logical access to systems must be restricted to authorised personnel and limited to the minimum level of access necessary for the performance of their functions, in accordance with the principle of least privilege.

9. PROTECTION OF INFORMATION

9.1 A banking institution or a microfinance banking institution must:

(a) Implement a data lifecycle management policy or a similar relevant policy to classify, map and track all sensitive data from creation to disposal, with classifications reviewed at least twice a year, in accordance with the nature, size, complexity and risk profile of the banking institution or microfinance banking institution.

(b) Enforce least privilege access controls throughout the data lifecycle, supported by automated monitoring mechanisms to detect and respond to unauthorised access attempts. Access reviews must be conducted quarterly or more frequently, in line with zero trust principle depending on the banking institution or the microfinance banking institution's risk profile.

(c) Ensure that access is restricted solely to personnel with a legitimate business need and aligned with their job responsibilities, in accordance with the principle of least privilege.

(d) Establish retention schedules and secure disposal methods, including cryptographic erasure, for data no longer needed.

(e) Ensure that appropriate information security measures, based on its risk profile, are implemented to protect data at rest, in transit and in use. This may include, where appropriate, encryption, key management and other relevant security controls.

9.2 A banking institution or a microfinance banking institution must secure networks against unauthorised access and sophisticated attacks using effective, risk-based measures. Where data is transmitted across open or public networks, the banking institution must implement appropriate controls such as encryption, tokenisation or masking to protect the confidentiality and integrity of the data and in accordance with industry best practice standards.

9.3 A banking institution or a microfinance banking institution must maintain accurate network diagrams and data flow charts to ensure all connections and devices are identified and secured as well as to demonstrate how data moves across networks and between systems.

9.4 A banking institution or a microfinance banking institution must protect its information against malicious programs through proactive and responsive measures.

9.5 A banking institution or microfinance banking institution must implement appropriate measures to protect data at rest, data in motion and data in use, in relation to the criticality and sensitivity of the information. This must include data lifecycle policies that ensure secure handling from creation to disposal, with encryption and authentication tailored to data sensitivity.

10. DETECTION OF THREATS AND VULNERABILITIES

10.1 A banking institution or a microfinance banking institution must embed security measures into technology lifecycles to anticipate and counter evolving threats. Risks must be assessed, mitigated and monitored to ensure systems meet business and security requirements while maintaining adaptability to evolving threats.

10.2 A banking institution or a microfinance banking institution must ensure that employees at all levels can identify and report information security risks, with training suited to the threat landscape.

10.3 A banking institution or a microfinance banking institution must maintain accurate and reliable records of system activities for at least one year for critical systems, to support security monitoring and incident analysis.

10.4 A banking institution or a microfinance banking institution must establish a comprehensive testing program to validate the effectiveness of all elements of its framework. The results of the testing program should be used to support the ongoing improvement of its information security program.

10.5 At a minimum, penetration testing on critical systems must be performed at least annually or on a more frequent basis in alignment with the risk profile of the banking institution or microfinance banking institution.

10.6 A banking institution or microfinance banking institution must perform vulnerability assessments regularly to identify and assess security vulnerabilities in its systems and processes. The banking institution or microfinance banking institution must establish a process to prioritise and remedy issues identified in vulnerability assessments and perform subsequent validation to assess whether gaps have been fully addressed.

10.7 A banking institution or microfinance banking institution's vulnerability scans must be performed using automated vulnerability scanning software or a commercial vulnerability scanning service and restricted to a limited number of authorised individuals. Technical vulnerabilities must be remediated through appropriate risk based corrective measures such as patch management, or as per the banking institution or microfinance banking institution's vulnerability management practices.

10.8 A banking institution or a microfinance banking institution must conduct internal and external network vulnerability assessments scans on a periodic, risk-based basis or after any material changes in the network used by the banking institution or microfinance banking institution.

10.9 A banking institution or a microfinance banking institution must identify and document internal and external vulnerabilities. The likelihood of an occurrence, potential business impact and applicable risk responses must clearly be identified and documented.

10.10 A banking institution or a microfinance banking institution must establish and maintain cyber threat intelligence capabilities to collect, analyze and monitor cyber and fraudrelated information relevant to its business functions, detect internal and external threats, and participate in trusted information-sharing arrangements with external parties to ensure actionable intelligence on information, fraud, and cyber threats, vulnerabilities and incidents.

11. INCIDENT RESPONSE AND RECOVERY

11.1 In the event that the information security of the banking institution or the microfinance banking institution is breached in any way, a banking institution or a microfinance banking institution must perform a thorough investigation to determine its nature and impact, as well as the damage inflicted. While the investigation is ongoing, the banking institution or microfinance banking institution must take immediate action to contain the situation to prevent further damage and commence recovery efforts to restore operations based on its incident recovery plan.

11.2 A banking institution or microfinance banking institution must maintain plans to respond to, contain, and recover from incidents and ensure rapid restoration of critical operations and services with adaptive capacity to handle systemic or cascading failures to enable the safe resumption of critical operations. These plans should outline the internal and external parties that must be notified of an information security or cyber incident, when a notification must occur and what information needs to be included in the notification. The plan should include clearly defined roles and responsibilities for all staff involved in cyber incident escalation, response and recovery, across all teams and departments within the banking institution or a microfinance banking institution and ensure that the staff responsible for responding to information and cyber incidents and breaches have the required skills and training to address the situation appropriately.

11.3 A banking institution or a microfinance banking institution must maintain and test data backup and restoration procedures regularly or at least quarterly. The banking institution or a microfinance banking institution must design and test its systems and processes to enable the safe resumption of critical operations within the industry.

11.4 A banking institution or a microfinance banking institution must regularly review and test its response and incident recovery plan, using a range of different scenarios and conduct simulation tests at least twice a year to ensure its continued effectiveness. The banking institution or microfinance banking institution should work together with its interconnected entities to enable the resumption of operations, as soon as it is safe and practical to do so without causing unnecessary risk to the wider sector or to financial stability.

11.5 A banking institution or a microfinance banking institution must have processes and procedures in place to conduct post-incident analysis to identify root causes of information security incidents and integrate findings into the response and recovery plans.

PART IV
REPORTING REQUIREMENTS

12. INCIDENT REPORTING

12.1 A banking institution or a microfinance banking institution must immediately, upon becoming aware of material information relating to an information or cyber security incident, report to the Director of Banking Supervision Department at the Bank through telephone or in writing, followed by regular updates until the incident is contained.

12.2 The banking institution or microfinance banking institution must communicate with internal and external parties to ensure a coordinated response to incidents, as well as determine the type of information to be reported, to whom such information should be reported, and when such information should be reported.

12.3 The banking institution or a microfinance banking institution or microfinance banking institution must report all material information and cyber incidents to the Bank. The banking institution or microfinance banking institution must consider an information security incident material as guided in Annexure A and Table 1 below.

12.4 A banking institution or a microfinance banking institution must classify material information security incidents as those that fulfil:

(a) One or more criteria for the higher impact level, or

(b) Three or more criteria at the lower impact level, as set out in Table 1 and Annexure A of this Determination.

12.5 A banking institution or a microfinance banking institution must subsequently submit information related to the incident in a form to be issued by the Bank. The submission must be made within 24 hours after detecting the incident or the next immediate working day in case the incident occurred on weekends and public holidays.

12.6 A banking institution or microfinance banking institution must assess an information and cyber security incident against the following criteria and their underlying indicators:

(a) Transactions affected - the banking institution or microfinance banking institution must determine the total value of the transactions affected, as well as the number of payments compromised as a percentage of the regular level of payment transactions carried out with the affected payment services.

(b) Users affected - the banking institution or microfinance banking institution must determine the number of clients affected, both in absolute terms and as a percentage of the total number of service users.

(c) Service downtime - the banking institution or microfinance banking institution must determine the period of time when the service will probably be unavailable for the service user.

(d) Economic impact - the banking institution or microfinance banking institution must determine the monetary costs associated with the incident holistically and take into account both the absolute figure and, when applicable, the relative importance of these costs in relation to the size of the banking institution or microfinance banking institution.

(e) Escalation of incident reporting - the banking institution or microfinance banking institution must indicate whether the incident has been escalated to senior or executive management within the banking institutions or microfinance banking institution.

(f) Other institutions or relevant infrastructures potentially affected - The banking institution or microfinance banking institution must assess whether the incident could have systemic implications, including whether it may impact other banking institutions, financial market infrastructures, and payment services industry. The outcome of this assessment must be included in the incident-reporting form to be submitted to the Bank.

(g) Reputational impact - A banking institution or microfinance banking institution must assess whether the incident could undermine users' trust in the institution, the affected service or the broader market. The outcome of this assessment must be included in the incident-reporting form to be submitted to the Bank.

12.7 A banking institution or microfinance banking institution must assess an incident by determining, for each criterion, whether the relevant thresholds in Table 1 below have been met or are likely to be met before the incident is resolved.

Table 1: Material Information Security Incidents Thresholds

Criteria	**Lower impact level**	**Higher impact level**
Transactions affected	> 10% of the banking institution or microfinance banking institution's regular level of transactions (in terms of number of transactions) and > N$10,000	> 25% of the banking institution or microfinance banking institution's regular level of transactions (in terms of number of transactions) or > N$500,000
Users affected	> 5 000 and > 10% of the banking institution's service users	> 50 000 or > 25% of the banking institution or microfinance banking institution's service users
Service downtime	< 2 hours	Not applicable (service downtime alone is not sufficient to determine a higher impact level in terms of Annexure A.)
Economic impact	Not applicable	> 0.1% *Common Equity Tier 1 capital* (CET 1)
Escalation of incident reporting	Yes	Yes, and a crisis mode (or equivalent) is likely to be called upon
Other institutions or relevant infrastructures are potentially affected	Yes – Within the group of related/affiliated institutions	Yes – External/third-party institutions
Reputational impact	Yes (affected clients or third parties, no media/public disclosure)	Yes (e.g., public/media disclosure)

12.8 The banking institution or microfinance banking institution must carry out the assessment referred to in section 12.8 on a continuous basis during the lifetime of the information and cyber security incident to identify any possible status change, either upwards (from nonmaterial to material) or downwards (from material to non-material).

PART V
ANCILLARY MATTERS

13. CORRECTIVE MEASURES

13.1 Any contravention or failure to comply with any provisions of this Determination will be subjected to administrative penalties as contemplated in section 94(1) of the Act.

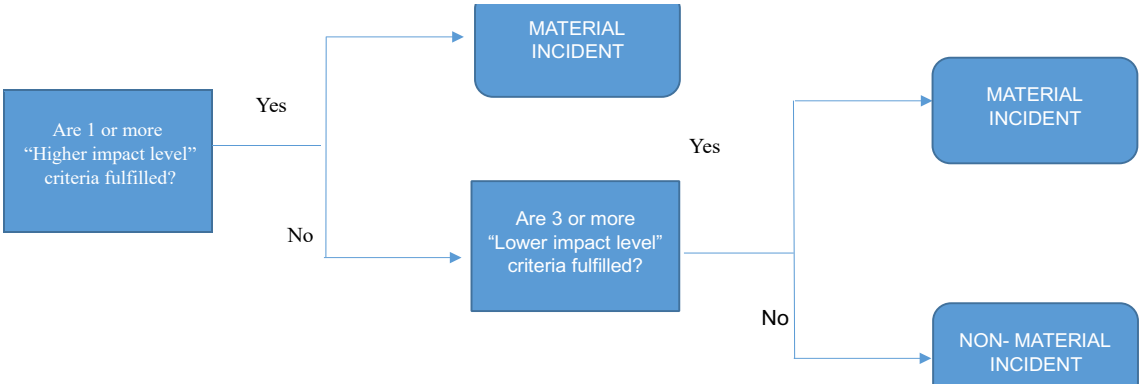
PART VI
EFFECTIVE DATE

14. The Determination comes into effect six months after the date of publication in the *Gazette*.

15. This Determination repeals the Determinations on Information Security (BID-30) published in the Government Gazette as a General Notice No. 6448 of 24 October 2017.

ANNEXURE A

DECISION TREE FOR ASSESSING WHETHER OR NOT AN INFORMATION SECURITY INCIDENT IS MATERIAL



Legend:

1. If an incident meets or is likely to meet one or more higher impact level thresholds, it qualifies as material.

2. If an incident does not meet and is unlikely to meet any higher impact level threshold but meets or is likely to meet 3 or more 'Lower impact level' thresholds, it qualifies as material.

3. If an incident does not meet and will likely not meet any higher impact level thresholds and does not meet and will likely not meet at least three lower impact level thresholds, it does not qualify as material