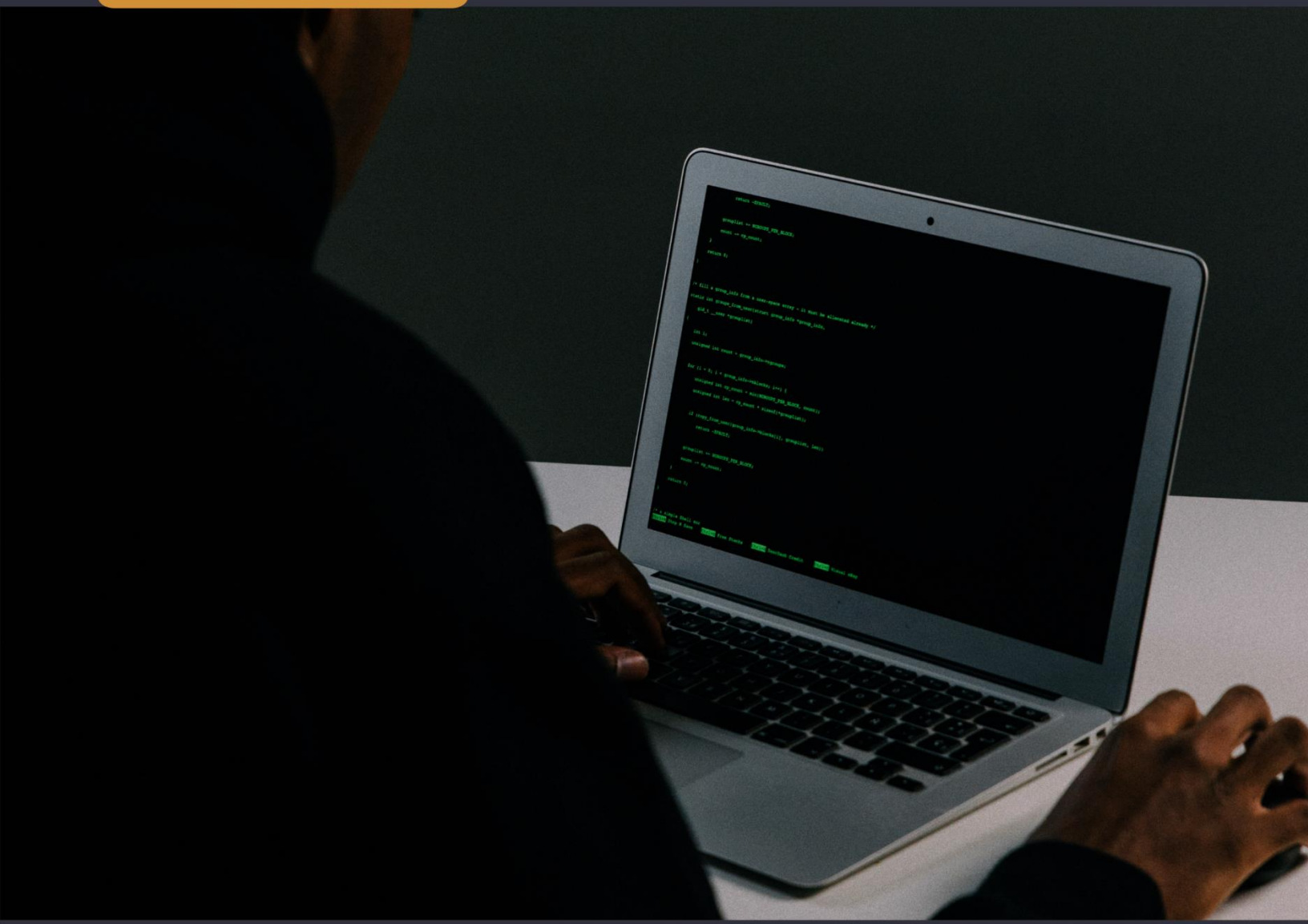
CBE GUIDELINES ON CYBERSECURITY FOR FINANCIAL INSTITUTIONS No. 1 of 2021

JANUARY 2021



CENTRAL BANK OF ESWATINI

Umntsholi Wemaswati

TABLE OF CONTENTS

1. Introduction, Citation and Commencement

1.1. Introduction

1.1.1. These Guidelines shall be referred to as the *CBE Cybersecurity Guidelines for Financial Institutions No. 1 of 2021* and shall come into force on 1 March 2021, and are hereby issued by the Central Bank Governor.

1.1.2. The cybersecurity guidelines have been issued by the Central Bank (herein referred to as the Bank) in exercise of powers conferred to it by sections 4 (f), 4 (g) and 42 (b) of the Central Bank of Swaziland Order 1974 (as amended). In terms of this legislation, the Bank is required to promote, regulate and supervise the efficient and secure operation of payment systems to the end of promoting a sound national financial structure; and to supervise clearing houses and other organized systems for the making of payments.

1.1.3. The cybersecurity guidelines have been issued to manage cyber risks facing ICT systems that financial institutions are reliant on. The guidelines are based on the *Guidance on cyber resilience for financial market infrastructures*[1] published in 2016 by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO). The Bank has customised and adopted the guidance for implementation in Eswatini.

1.1.4. This Guidance is presented in chapters that outline five primary risk management categories and three overarching components that should be addressed across an Financial Institutions' cyber resilience framework. The risk management categories are: (i) governance; (ii) identification; (iii) protection; (iv) detection; and (v) response and recovery. The overarching components are: (i) testing; (ii) situational awareness; and (iii) learning and evolving, see figure below.

[1] Available at https://www.bis.org/cpmi/publ/d146.pdf

Figure 1. Cyber resilience guidance components

1.2. Purpose

1.2.1. The purpose of this document is to outline measures that financial institutions regulated and licensed by the Central Bank should put in place to enhance their cyber resilience.

1.3. Applicability

1.3.1. All financial institutions regulated and licensed by the Central Bank under the Financial Institutions Act, 2005, Exchange Control Order, 1974, and National Clearing and Settlement Systems Act, 2011 (herein referred to as *the Acts*) are expected to implement the guidelines within 12 months of their publication.

1.4. Oversight

1.4.1. The Bank shall conduct oversight inspections and examinations on financial institutions to assess the adequacy of cyber resilience. The inspections and examinations would be based on the requirements provided in *the Acts* and these Guidelines and other assessment processes, developed from time to time.

2. Interpretations

In this Guideline:

Actionable intelligence	Information that can be acted upon to address, prevent or mitigate a cyber threat.
Attack surface	The sum of an information system's characteristics in the broad categories (software, hardware, network, processes and human) which allows an attacker to probe, enter, attack or maintain a presence in the system and potentially cause damage to a financial institution. A smaller attack surface means that the financial institution is less exploitable and an attack less likely. However, reducing attack surfaces does not necessarily reduce the damage an attack can inflict.
Availability	The property of being accessible and usable as expected upon demand.
Business process	A collection of linked activities that takes one or more kinds of input and creates an output that is of value to a financial institution's stakeholders. A business process may comprise several assets, including information, ICT resources, personnel, logistics and organisational structure, which contribute either directly or indirectly to the added value of the service.
Critical operations	Any activity, function, process, or service, the loss of which, for even a short period of time, would materially affect the continued operation of a financial institution, its participants, the market it serves, and/or the broader financial system.
Cyber	Refers to the interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.
Cyber attack	An assault launched by an adversary using computer technology to exploit vulnerabilities in a computer or networks with malicious intent of achieving an adverse effect on the ICT environment.
Cyber event	An observable occurrence in an information system or network.
Cyber governance	Arrangements an organisation puts in place to establish, implement and review its approach to managing cyber risks.

Cyber maturity model	A mechanism to have cyber resilience controls, methods and processes assessed according to management best practice, against a clear set of external benchmarks.
Cyber resilience	A financial institution's ability to anticipate, withstand, contain and rapidly recover from a cyber attack.
Cyber resilience framework	Consists of the policies, procedures and controls a financial institution has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces.
Cyber resilience strategy	A financial institution's high level principles and medium term plans to achieve its objective of managing cyber risks.
Cyber risk	The combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for an organisation.
Cyber risk management	The process used by a financial institution to establish an enterprise-wide framework to manage the likelihood of a cyber attack and develop strategies to mitigate, respond to, learn from and coordinate its response to the impact of a cyber attack. The management of a financial institution's cyber risk should support the business processes and be integrated in the financial institution's overall risk management framework.
Cyber risk profile	The cyber risk actually assumed, measured at a given point in time.
Cyber risk tolerance	The propensity to incur cyber risk, being the level of cyber risk that a financial institution intends to assume in pursuing its strategic objectives.
Cyber threat	A circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a financial institution's systems, resulting in a loss of confidentiality, integrity or availability.
Cyber threat intelligence	Information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event (may also be referred to as "cyber threat information").
Defence in depth	The security controls deployed throughout the various layers of the network to provide for resiliency in the event of the failure or the exploitation of a vulnerability of another control (may also be referred to as "layered protection").

Detection	Development and implementation of the appropriate activities in order to identify the occurrence of a cyber event.
Disruption	A disruption is an event affecting an organisation's ability to perform its critical operations.
Ecosystem	A system or group of interconnected elements, formed linkages and dependencies. For a financial institution, this may include participants, linked financial institutions, service providers, vendors and vendor products.
Financial institution	Any institution licensed in terms of the Financial Institutions Act, 2005 or regulated by the Central Bank.
Financial market infrastructure	A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions.
Forensic investigation	The application of investigative and analytical techniques to gather and preserve evidence from a digital device impacted by a cyber attack.
Forensic readiness	The ability of a financial institution to maximise the use of digital evidence to identify the nature of a cyber attack.
ICT	Information and communications technologies. ICT can also be read as IT (information technology) in this document.
Identification	To develop the organisational understanding required to manage cyber risk to systems, assets, data and capabilities.
Indicator	An occurrence or sign which reveals that an incident may have occurred or be in progress.
Information Asset	Any piece of data, device or other component of the environment that supports information-related activities. In the context of this report, information assets include data, hardware and software. Information assets are not limited to those that are owned by the entity. They also include those that are rented or leased, and those that are used by service providers to deliver their services.
Integrity	With reference to information, an information system or a component of a system, the property of not having been modified or destroyed in an unauthorised manner.
Layered Protection	As relying on any single defence against a cyber threat may be inadequate, a financial institution can use a series of different

	defences to cover the gaps in and reinforce other protective measures. For example, the use of firewalls, intrusion detection systems, malware scanners, integrity auditing procedures and local storage encryption tools can serve to protect information assets in a complementary and mutually reinforcing manner. May also be referred to as "defence in depth".
Leading Standards, Guidelines And Practices	Standards, guidelines and practices which reflect industry best approaches to managing cyber threats, and which incorporate what are generally regarded as the most effective cyber resilience solutions.
Malware	Malicious software used to disrupt the normal operation of an information system in a manner that adversely impacts its confidentiality, availability or integrity.
Operational Resilience	The ability of a financial institution to: (i) maintain essential operational capabilities under adverse conditions or stress, even if in a degraded or debilitated state; and (ii) recover to effective operational capability in a time frame consistent with the provision of critical economic services.
Protection	Development and implementation of appropriate safeguards, controls and measures to enable reliable delivery of critical infrastructure services.
Recover	To restore any capabilities or services that have been impaired due to a cyber event.
Red Team	An independent group that challenges the cyber resilience of an organisation to test its defences and improve its effectiveness. A red team views the cyber resilience of a financial institution from an adversary's perspective.
Resilience By Design	The embedding of security in technology and system development from the earliest stages of conceptualisation and design.
Respond	Of a financial institution, to develop and implement appropriate activities to be able to take action when it detects a cyber event.
Resume	To recommence functions following a cyber incident. A financial institution should resume critical services as soon as it is safe and practicable to do so without causing unnecessary risk to the wider sector or further detriment to financial stability.

	The plan of action should incorporate the use of a secondary site and be designed to ensure that critical ICT systems can resume operations within two hours following a disruptive event.
Risk-Based Approach	An approach whereby financial institutions identify, assess and understand the risks to which they are exposed to and take measures commensurate with these risks.
Risk Tolerance	The amount and type of risk that an organisation is willing to take in order to meet its strategic objectives (may also be referred to as "risk appetite").
Security Operations Centre	A function or service responsible for monitoring, detecting and isolating incidents.
Situational Awareness	The ability 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.
Threat	A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organisational operations, organisational assets (including information and information systems), individuals, other organisations or society in general.
Transaction Replay	To execute a transaction that had been previously executed. Replaying is normally performed when data is restored using a backup taken at an earlier time than the transactions being replayed.
Vulnerability	A weakness, susceptibility or flaw in a system that an attacker can access and exploit to compromise system security. Vulnerability arises from the confluence of three elements: the presence of a susceptibility or flaw in a system; an attacker's access to that flaw; and an attacker's capability to exploit the flaw.

3. Governance

3.1. Preamble

3.1.1. Cyber governance refers to the arrangements a financial institution has put in place to establish, implement and review its approach to managing cyber risks. Effective cyber governance should start with a clear and comprehensive cyber resilience framework that prioritises the security and efficiency of the financial institution's operations, and supports financial stability objectives.

3.1.2. The framework should be guided by a financial institution's cyber resilience strategy, define how the financial institution's cyber resilience objectives are determined, and outline its people, processes and technology requirements for managing cyber risks and timely communication, in order to enable a financial institution to collaborate with relevant stakeholders to effectively respond to and recover from cyber attacks.

3.1.3. It is essential that the framework is supported by clearly defined roles and responsibilities of the financial institution's board (or equivalent) and its management, and it is incumbent upon its board and management to create a culture which recognises that staff at all levels have important responsibilities in ensuring the financial institution's cyber resilience.

3.1.4. Strong cyber governance is essential to a financial institution's implementation of a systematic and proactive approach to managing the prevailing and emerging cyber threats that it faces. It also supports efforts to appropriately consider and manage cyber risks at all levels within the organisation and to provide appropriate resources and expertise to deal with these risks.

3.1.5. This chapter provides guidance on what basic elements a financial institution's cyber resilience framework should include and how a financial institution's governance arrangements should support that framework.

3.2. Cyber resilience framework

3.2.1. A financial institution should have a framework that clearly articulates how it determines its cyber resilience objectives and cyber risk tolerance, as well as how it effectively identifies, mitigates, and manages its cyber risks to support its objectives.

The financial institution's board should endorse this framework, ensuring it is aligned with the financial institution's formulated cyber resilience strategy. The financial institution's cyber resilience framework should support financial stability objectives while ensuring the ongoing efficiency, effectiveness and economic viability of its services to its users. Therefore, framework objectives should aim to maintain and promote the financial institution's ability to anticipate, withstand, contain and recover from cyber attacks, so as to limit the likelihood or impact of a successful cyber attack on its operations or on the broader financial system. The financial institution's cyber resilience framework should be reviewed and updated periodically to ensure that it remains relevant.

3.2.2. Cyber is more than just ICT. The strategies and measures in a financial institution's cyber resilience framework should not be restricted to securing the viability of its information technology operations alone, but should also cover people and processes. The framework should, in addition, include timely communication to enable the financial institution to collaborate with relevant stakeholders to effectively respond to and recover from cyber attacks, whether on the financial institution or on the financial system as a whole.

3.2.3. At the broader level, the financial institution's cyber resilience framework should be consistent with its enterprise operational risk management framework. Such consistency is important, and recognises that a financial institution's cyber resilience framework is likely to share common elements with the policies, procedures and controls that it has established to manage other areas of risks. For example, limiting physical access can be a key control to address the risk to critical ICT infrastructure.

3.2.4. A financial institution should take an integrated and comprehensive view of the potential cyber threats it faces. In particular, a financial institution's cyber resilience framework should consider how the financial institution would regularly review and actively mitigate the cyber risks that it bears from and poses to its participants, other financial institutions, vendors, vendor products and its service providers, which are collectively referred to in this document as a financial institution's ecosystem.

3.2.5. There are many relevant international, national and industry-level standards, guidelines or recommendations that a financial institution could use as a benchmark in designing its cyber resilience framework. Given financial institutions' systemic importance, they should align themselves with leading standards, guidelines or recommendations,

reflecting current industry best approaches in managing cyber threats, and incorporate the most effective cyber resilience solutions.

3.2.6. There are also other standards, guidelines or recommendations that the Central Bank shall require from time to time financial institutions to align with completely and the compliance be verified as part of the oversight of these guidelines.

3.2.7. A financial institution's cyber resilience framework should clearly define the roles and responsibilities including accountability for decision making within the organisation for managing cyber risk, including in emergencies and in a crisis.

3.2.8. A financial institution's internal processes should help the board and senior management assess and measure the adequacy and effectiveness of the financial institution's cyber resilience framework. The adequacy of and adherence to a financial institution's cyber resilience framework should be assessed and measured regularly through independent compliance programmes and audits carried out by qualified individuals. To assess and measure the effectiveness of its cyber resilience framework, a financial institution is encouraged to use relevant metrics and maturity models as well as the results of its testing programme.

3.3. Role of the board and senior management

3.3.1. A financial institution's board is ultimately responsible for setting the cyber resilience framework and ensuring that cyber risk is effectively managed. The Board should endorse the financial institution's cyber resilience framework, and set the financial institution's tolerance for cyber risk. The board should be regularly apprised of the financial institution's cyber risk profile to ensure that it remains consistent with the financial institution's risk tolerance as well as the financial institution's overall business objectives. As part of this responsibility, the board should consider how material changes to the financial institution's products, services, policies or practices, and the threat landscape affect its cyber risk profile. Senior management should closely oversee the financial institution's implementation of its cyber resilience framework, and the policies, procedures and controls that support it.

3.3.2. A financial institution's board and senior management should cultivate a strong level of awareness of and commitment to cyber resilience. To that end, a financial institution's board and management should promote a culture that recognises that staff at all levels have important responsibilities in ensuring the financial institution's cyber resilience, and lead by example.

3.3.3. In order for the board and senior management to have effective oversight of the financial institution's cyber resilience framework and cyber risk profile, both groups should contain members with the appropriate skills and knowledge to understand and manage the risks posed by cyber threats, while ensuring that those skills remain current.

3.3.4. In view of financial institutions' growing reliance on ICT systems to support their businesses and operations, and the increasing cyber threat, financial institutions should designate a senior executive to be responsible and accountable for executing the cyber resilience framework within the organisation. This role should have sufficient authority, independence, resources and access to the board. The senior executive performing this role should possess the requisite expertise and knowledge to competently plan and execute the cyber resilience initiatives.

4. Identification

4.1. Preamble

4.1.1. Given that a financial institution's operational failure can negatively impact financial stability, it is crucial that financial institutions identify which of their critical operations and supporting information assets should, in order of priority, be protected against compromise. The ability of a financial institution to understand its internal situation and external dependencies is key to being able to effectively respond to potential cyber threats that might occur. This requires a financial institution to know its information assets and understand its processes, procedures, systems and other dependencies to strengthen its overall cyber resilience posture.

4.1.2. This chapter outlines areas where a financial institution should identify and classify business processes and information assets as well as external dependencies.

4.2. Identification and classification

4.2.1. A financial institution should identify its business functions and supporting processes and conduct a risk assessment in order to ensure that it thoroughly understands the importance of each function and supporting processes, and their interdependencies, in performing its functions. Identified business functions and processes should then be classified in terms of criticality, which in turn should guide the financial institution's prioritisation of its protective, detective, response and recovery efforts.

4.2.2. Similarly, a financial institution should identify and maintain a current inventory of its information assets and system configurations, including interconnections with other internal and external systems, in order to know at all times the assets that support its business functions and processes. A financial institution should carry out a risk assessment of those assets and classify them in terms of criticality. It should identify and maintain a current log of both individual and system usernames to know the access rights to information assets and their supporting systems, and should use this information to facilitate identification and investigation of anomalous activities.

4.2.3. A financial institution should integrate identification efforts with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its list of critical business processes, functions, individual and system credentials and its inventory of information assets so that that they remain current, accurate and complete.

4.3. Interconnections

4.3.1. A financial institution's systems and processes are directly or indirectly interconnected with the systems and processes of the entities within its ecosystem, e.g. participants, linked financial institutions, settlement banks, liquidity providers, service providers, critical infrastructure such as energy and telecommunications, vendors and vendor products.

4.3.2. Consequently, the cyber resilience of those entities could have significant implications in terms of the cyber risk that the financial institution faces, particularly since the significance of the risks they may pose is not necessarily proportionate to the criticality of their business relationship with the financial institution.

4.3.3. Therefore, a financial institution should identify the cyber risks that it bears from and poses to entities in its ecosystem and coordinate with relevant entities, as appropriate, as they design and implement resilience efforts with the objective of improving the overall resilience of the ecosystem.

5. Protection

5.1. Preamble

5.1.1. Cyber resilience depends on effective security controls and system and process design that protect the confidentiality, integrity and availability of a financial institution's assets and services. These measures should be proportionate to a financial institution's threat landscape and systemic role in the financial system, and consistent with its risk tolerance.

5.1.2. This chapter provides guidance on how financial institutions should implement appropriate and effective measures in line with leading cyber resilience and information security practices to prevent, limit or contain the impact of a potential cyber event.

5.2. Protection of processes and assets

5.2.1. A financial institution should implement appropriate protective controls that are in line with leading-practice cyber resilience standards to minimise the likelihood and impact of a successful cyber attack on identified critical business functions, information assets and data. Protective controls should be proportionate to the financial institution's threat landscape and systemic role in the financial system, and consistent with its risk tolerance.

5.2.2. A financial institution should consider cyber resilience from the ground up during system, process, and product design. A process to instil resilience by design should ensure that, among other measures, software, network configurations, and hardware supporting or connected to critical systems are subject to rigorous testing against related security standards, that attack surfaces are limited to the extent practicable, and that common information security principles relating to confidentiality, integrity and availability are adhered to (e.g., ensuring that access to systems is restricted to those with a legitimate business requirement).

5.2.3. Financial institutions should consistently maintain a strong ICT control environment, this being a fundamental and critical component of a financial institution's overall cyber resilience. While ICT controls are not the focus of this guidance, a few important but non-exhaustive examples are provided below:

a. Protecting information. Implementing appropriate measures to protect information (both in transit and at rest), commensurate with the criticality and sensitivity of the information held by and transmitted through the financial institution. This should include, but not be restricted to, appropriate encryption (e.g., end-to-end encryption), authentication (e.g., multifactor authentication) and access control.

b. Change management. Ensuring that the financial institution has a comprehensive change management process that explicitly considers cyber risks, in terms of residual cyber risks identified both prior to and during a change, and of any new cyber risk created post-change. Ensuring that a process exists to identify patches to technology and software assets, evaluate the patch criticality and risk, and test and apply the patch within an appropriate time frame.

c. Security settings consistent with levels of protection. Configuring ICT systems and devices with security settings that are consistent with the expected level of protection. Financial institutions should establish baseline system security configuration standards to facilitate consistent application of security settings to operating systems, databases, network devices and enterprise mobile devices within the ICT environment. Regular enforcement checks should also be performed to ensure that non-compliance with such standards is promptly rectified.

5.2.4. A financial institution's protective controls should enable the monitoring and detection of anomalous activity across multiple layers of the financial institution's infrastructure, which requires a baseline profile of system activity. Controls should be implemented in a way that will assist in monitoring for, detecting, containing and analysing anomalous activities should protective measures fail. For example, (re-)designing processes to introduce more segmentation, intermediate checkpoints and intermediate reconciliations may allow quicker detection, identification and repair/recovery from a disruption.

5.2.5. Similarly, segmenting networks in a manner that segregates systems and data of varying criticality may have multiple benefits, both by helping the financial institution to

insulate systems in one segment from a security compromise in other segments, and by facilitating more efficient recovery of services. The latter benefit is achieved because, in the event of such a compromise, only the affected segments have to be restored, rather than the entire ICT infrastructure and all data sets.

5.3. Interconnections

5.3.1. A financial institution should implement protective measures to mitigate risks arising from the entities within its ecosystem. The appropriate controls for each entity will depend on the risk that arises from the connected entity and the nature of the relationship with the entity. In view of its systemic importance and unique position in the financial system, a financial institution should implement measures to mitigate effectively the risk arising from its connected entities, including the following:

a. A financial institution's participation requirements should be designed to ensure that they adequately support its cyber resilience framework.
b. The financial institution's framework to manage its relationship with service providers should address and be designed to mitigate cyber risks. At a minimum, a financial institution should ensure that its outsourced services are accorded the same level of cyber resilience needed if their services were provided by the financial institution itself.
c. Cyber considerations should be integral part of the financial institution's arrangements for managing vendors and vendor products in the areas of contracts, performance, relationships and risk. Contractual agreements between the financial institution and its service providers should ensure that the financial institution and relevant authorities are provided with or have full access to the information necessary to assess the cyber risk arising from the service provider.

5.4. Insider threats

5.4.1. A financial institution should implement measures to capture and analyse anomalous behaviour by persons with access to its systems. Data loss identification and prevention techniques should be employed to protect against the removal of confidential data from the financial institution's network.

5.4.2. A financial institution should conduct screening/background checks on new employees to mitigate insider threats. Similar checks should be conducted on all staff at regular intervals throughout their employment, commensurate with staff's access to critical

systems. Financial institutions also should establish processes and controls to mitigate risks related to employees terminating employment or changing responsibilities.

5.4.3. Physical and logical access to systems should be permitted only for individuals who are authorised, and authorisation should be limited to individuals who are appropriately trained and monitored. Financial institutions should institute controls that reliably restrict such access to systems to those with a legitimate business requirement. In particular, financial institutions should institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as roles-based access, logging and reviewing of the systems activities of privileged users, strong authentication, and monitoring for anomalies should be implemented.

5.5. Training

5.5.1. A financial institution should ensure that all relevant staff, be they permanent or temporary, receive training at least once a year to develop and maintain appropriate awareness of and competencies for detecting and addressing cyber-related risks. They should also be trained on how to report any unusual activity and incidents.

5.5.2. High-risk groups, such as those with privileged system access or in sensitive business functions, should be identified and should receive targeted information security training.

6. Detection

6.1. Preamble

6.1.1. A financial institution's ability to recognise signs of a potential cyber incident, or detect that an actual breach has taken place, is essential to strong cyber resilience. Early detection provides a financial institution with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches. In the latter case, early containment could effectively mitigate the impact of the attack – for example, by preventing an intruder from gaining access to confidential data or exfiltration of such data.

6.1.2. Given the stealthy and sophisticated nature of cyber attacks and the multiple entry points through which a compromise could take place, a financial institution should maintain effective capabilities to extensively monitor for anomalous activities.

6.1.3. This chapter outlines monitoring- and process-related guidance aimed at helping financial institutions detect cyber incidents.

6.2. Detecting a cyber attack

6.2.1. A financial institution should establish capabilities to continuously monitor (in real time or near real time) and detect anomalous activities and events. One practice that may help to accomplish this is to set up what is commonly referred to as a "security operations centre". These capabilities should be adaptively maintained and tested.

6.2.2. A financial institution should monitor relevant internal and external factors, including business line and administrative functions and transactions. The financial institution should seek to detect both publicly known vulnerabilities and vulnerabilities that are not yet publicly known, such as so-called zero-day exploits, through a combination of signature monitoring for known vulnerabilities and behaviourally based detection mechanisms.

6.2.3. Detection capabilities should also address misuse of access by service providers or other trusted agents, potential insider threats and other advanced threat activity. These processes should be informed by and integrated with a strong cyber threat intelligence programme (see paragraphs 9.2.1 and 9.2.2 below).

6.2.4. The ability to detect an intrusion early is critical for swift containment and recovery. Financial institutions should take a defence-in-depth approach by instituting multi-layered detection controls covering people, processes and technology, with each layer serving as a safety net for preceding layers.

6.2.5. As a cyber attack typically progresses in a sequence of stages before attaining its end objective, financial institutions should also apply approaches that enable them to delay or disrupt the attackers' ability to advance within the attack sequence. In addition, an effective intrusion detection capability could assist financial institutions in identifying deficiencies in their protective measures for early remediation.

6.2.6. A financial institution's monitoring and detection capabilities should facilitate its incident response process and support information collection for the forensic investigation process.

6.2.7. A financial institution should implement measures to capture and analyse anomalous behaviour by persons with access to the financial systems network.

7. Response and recovery

7.1. Preamble

7.1.1. Financial stability may depend on a financial institution's ability to settle obligations when they are due. Therefore, a financial institution's arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data in order to mitigate the potentially systemic risks of failure to meet such obligations when participants are expecting it to meet them. Continuity planning is essential in meeting related objectives.

7.1.2. This chapter provides guidance on a financial institution's capabilities to respond to and recover from cyber attacks.

7.2. Incident response, resumption and recovery

7.2.1. Upon detection of a successful cyber attack or an attack attempt, financial institutions should perform a thorough investigation to determine its nature and extent as well as the damage inflicted. While the investigation is ongoing, financial institutions should also take immediate actions to contain the situation to prevent further damage and commence recovery efforts to restore operations based on their response planning.

7.2.2. Objectives for resuming operations set goals for, ultimately, the sound functioning of the financial system, which should be planned for and tested against. A financial institution should, design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios.

7.2.3. Notwithstanding this capability to resume critical operations within two hours, financial institutions should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, while taking into account that completion of settlement by the end of day is crucial.

7.2.4. While financial institutions should plan to safely resume critical operations within two hours of a disruption, they should also plan for scenarios in which this objective is not achieved.

7.2.5. Financial institutions should analyse critical functions, transactions and interdependencies to prioritise resumption and recovery actions, which may, depending on the design of the financial institution, facilitate the processing of critical transactions, for example, while remediation efforts continue.

7.2.6. Financial institutions should also plan for situations where critical people, processes or systems may be unavailable for significant periods – for example, by potentially reverting, where feasible, safe and practicable, to manual processing if automated systems are unavailable.

7.2.7. Financial institutions should develop and test response, resumption and recovery plans. These plans should support objectives to protect and, if necessary, re-establish integrity and availability of its operations, and the confidentiality of its information assets.

7.2.8. Plans should be actively updated based on current cyber threat intelligence, information-sharing and lessons learned from previous events, as well as analysis of operationally and technically plausible scenarios that have not yet occurred. The financial institution should consult and coordinate with relevant internal and external stakeholders during the establishment of its response, resumption and recovery plans.

7.3. Design elements

7.3.1. System and process design and controls for critical functions and operations should support incident response activities to the extent possible. Financial institutions should design systems and processes to limit the impact of any cyber incident, resume critical operations within two hours of a disruption, complete settlement by day-end and preserve transaction integrity.

7.3.2. The possibility to resume critical operations in a system that is technically different from the primary system or in a system that performs those operations and completes settlement in a non-standardised way may be among the options for a financial institution to consider.

7.3.3. A financial institution's incident response, resumption and recovery processes should be closely integrated with crisis management, business continuity and disaster recovery planning and recovery operations, and coordinated with relevant internal and external stakeholders.

7.3.4. Financial institutions should have plans to identify, in a timely manner, the status of all transactions and member positions at the time of a disruption, supported by corresponding recovery point objectives. Therefore, financial institutions should design and test their systems and processes to enable recovery of accurate data following a breach.

7.3.5. Data instances should be safeguarded by stringent protective and detective controls. In addition, the financial institution's cyber resilience framework should include data

recovery measures, such as keeping a copy of all received and processed data (including the original intent of instructions being sent to the financial institution for processing), maintaining transaction replay capability and conducting frequent periodic independent reconciliation of participants' positions.

7.3.6. Recovery point objectives to support data integrity efforts should be consistent with the financial institution's resumption time objective for critical operations. Financial institutions should consider diverse approaches to achieving these objectives.

7.4. Interconnections

7.4.1. In the event of a successful cyber attack that compromises the integrity of a financial institution's data, a successful recovery may require sharing of data with third parties and/or participants to help with the investigation and disclosure. Financial institutions should consider setting up data-sharing agreements with relevant third parties or participants in advance in order to enable such data to be shared in a timely manner once a successful cyber attack has been identified.

7.4.2. Since a financial institution's systems and processes are often interconnected with the systems and processes of other entities within its ecosystem, in the event of a large-scale cyber incident it is possible for a financial institution to pose contagion risk (i.e., propagation of malware or corrupted data) to, or be exposed to contagion risk from, its ecosystem.

7.4.3. A financial institution should work together with its interconnected entities to enable the resumption of operations (the first priority being its critical services) as soon as it is safe and practicable to do so without causing unnecessary risk to the wider sector or further detriment to financial stability.

7.4.4. Financial institutions should plan in advance for communications with participants, interdependent financial institutions, authorities and others (such as service providers and, where relevant, the media). Communication plans should be developed through an adaptive process informed by scenario-based planning and analysis as well as prior experience. Because rapid escalation of cyber incidents may be necessary, financial institutions should determine decision-making responsibilities for incident response in advance, and implement clearly defined escalation and decision-making procedures.

7.4.5. Financial institutions should have a policy and procedure to enable the responsible disclosure of potential vulnerabilities. In particular, financial institutions should prioritise disclosures that could facilitate early response and risk mitigation by

stakeholders for the benefit of the ecosystem and broader financial stability, following the possible approaches outlined in paragraph 9.3.2 below.

7.4.6. Financial institutions should have the capability to conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative process. In this regard, financial institutions should establish relevant system logging policies that include the types of logs to be maintained and their retention periods.

7.4.7. While forensic analysis may need to be postponed, e.g. in the event of contagion giving rise to financial stability concerns, and ICT resources may be focused on recovering critical systems, financial institutions should take appropriate steps so that investigations can still be performed post-event to the extent possible, e.g. through preservation of necessary system logs and evidence.

7.5. Incident Notification

7.5.1. In the event of a successful cyber attack, a financial institution should notify the Central Bank within two hours of verifying the incident. The financial institution should be ready to provide updates on the incident which the Central Bank may request. See incident notification form in Appendix A.

7.5.2. Once a financial institution is satisfied that it has contained and recovered from an incident, it shall submit a report to the Central Bank. The report is expected at most on the fourth working days since the incident was detected. Should investigations not been complete, the report shall contain available information and a note that a full report shall be submitted at conclusions of investigations.

8. Testing

8.1. Preamble

8.1.1. Testing is an integral component of any cyber resilience framework. All elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within a financial institution, and regularly thereafter. This includes the extent to which the framework is implemented correctly, operating as intended and producing desired outcomes. Understanding the overall effectiveness of the cyber resilience framework in the financial institution and its environment is essential in determining the residual cyber risk to the financial institution's operations, assets, and ecosystem.

8.1.2. Sound testing regimes produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the financial institution's cyber risk management process. Analysis of testing results provides direction on how to correct weaknesses or deficiencies in the cyber resilience posture and reduce or eliminate identified gaps.

8.1.3. This chapter provides guidance on areas that should be included in a financial institution's testing and how results from testing can be used to improve the financial institution's cyber resilience posture on an ongoing basis. The scope of testing for the purpose of this guidance includes vulnerability assessments, scenario-based testing, penetration tests and tests using red teams.

8.2. Comprehensive testing programme

8.2.1. A financial institution should establish a comprehensive testing programme to validate the effectiveness of its cyber resilience framework on a regular and frequent basis. It should employ appropriate cyber threat intelligence to inform its testing methods – for example, by designing tests to simulate advanced threat agent capabilities and extreme but plausible scenarios.

8.2.2. The results of the testing programme should be used by the financial institution to support the ongoing improvement of its cyber resilience. Where applicable, these tests should include both internal and external stakeholders such as business line management including business continuity, incident and crisis response teams, and the relevant entities in its ecosystem.

8.2.3. A financial institution should involve its board and senior management appropriately (e.g., as part of crisis management teams) and inform them of test results.

8.2.4. Financial institutions should employ a variety of effective testing methodologies and practices, including the following (which may partly overlap or be combined):

a. Vulnerability assessment (VA). Financial institutions should regularly perform vulnerability assessments to identify and assess security vulnerabilities in their systems and processes. Financial institutions should establish a process to prioritise and remedy issues identified in VAs and perform subsequent validation to assess whether gaps have been fully addressed.

b. Scenario-based testing. A financial institution's response, resumption and recovery plans should be subject to periodic review and testing. Tests should address an appropriately broad scope of scenarios, including simulation of extreme but plausible cyber attacks, and should be designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans. Financial institutions should use cyber threat intelligence and cyber threat modelling to the extent possible to imitate the unique characteristics of cyber threats. They should also conduct exercises to test the ability of their staff and processes to respond to unfamiliar scenarios, with a view to achieving stronger operational resilience.

c. Penetration tests. Financial institutions should carry out penetration tests to identify vulnerabilities that may affect their systems, networks, people or processes. To provide an in-depth evaluation of the security of financial institutions' systems, those tests should simulate actual attacks on the systems. Penetration tests on internet-facing systems should be conducted regularly and whenever systems are updated or deployed. Where applicable, the tests could include other internal and external stakeholders, such as those involved in business continuity, incident and crisis response teams, as well as third parties, such as service providers and participants.

d. Red team tests. Financial institutions should challenge their own organisations and ecosystems through the use of so-called red teams to introduce an adversary perspective in a controlled setting. Red teams serve to test for possible vulnerabilities and the effectiveness of a financial institution's mitigating controls. A red team may consist of a financial institution's own employees and/or outside experts, who are in either case independent of the function being tested.

8.3. Coordination

8.3.1. A financial institution should, to the extent practicable and possible, promote, design, organise and manage exercises designed to test its response, resumption and recovery plans and processes. Such exercises should include financial institution participants, critical service providers and linked financial institutions.

8.3.2. Financial institutions should participate in exercises organised by the Central Bank and in industry-wide tests. Achieving market-wide timely recovery of operations calls for an added dimension to testing exercises. Traditional isolated testing implicitly assumes that all other players operate as usual. Removing that hypothesis helps a financial institution to identify plausible complexities, dependencies and weaknesses that may have been overlooked in its recovery plans. Accordingly, testing should include scenarios that cover breaches affecting multiple portions of the financial institution’s ecosystem.

9. Situational awareness

9.1. Preamble

9.1.1. Situational awareness refers to a financial institution's understanding of the cyber threat environment within which it operates, and the implications of being in that environment for its business and the adequacy of its cyber risk mitigation measures. Strong situational awareness, acquired through an effective cyber threat intelligence process can make a significant difference in the financial institution's ability to pre-empt cyber events or respond rapidly and effectively to them.

9.1.2. Specifically, a keen appreciation of the threat landscape can help a financial institution better understand the vulnerabilities in its critical business functions, and facilitate the adoption of appropriate risk mitigation strategies. It can also enable a financial institution to validate its strategic direction, resource allocation, processes, procedures and controls with respect to building its cyber resilience.

9.1.3. A key means of achieving situational awareness for a financial institution and its ecosystem is a financial institution's active participation in information-sharing arrangements and collaboration with trusted stakeholders within and outside the industry.

9.1.4. This chapter provides guidance for financial institutions to establish a cyber threat intelligence process, analysis and sharing processes.

9.2. Cyber threat intelligence

9.2.1. A financial institution should identify cyber threats that could materially affect its ability to perform or to provide services as expected, or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its ecosystem. In doing so, a financial institution should consider threats to the confidentiality, integrity and availability of the financial institution's business processes and to its reputation that could arise from internal and external sources. In addition, a financial institution should include in its threat analysis those threats which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. The financial institution should regularly review and update this analysis.

9.2.2. A financial institution should establish a threat intelligence process to gather and analyse relevant cyber threat information. Its analysis should be in conjunction with

other sources of internal and external business and system information so as to provide business-specific context, turning the information into usable cyber threat intelligence that provides timely insights and informs enhanced decision-making by enabling the financial institution to anticipate a cyber attacker's capabilities, intentions and modus operandi.

9.2.3. The scope of cyber threat intelligence gathering should include the capability to gather and interpret information about relevant cyber threats arising from the financial institution's participants, service and utility providers and other financial institutions, and to interpret this information in ways that allow the financial institution to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards in its systems. In this context, relevant cyber threat intelligence could include information on geopolitical developments that may trigger cyber attacks on any entity within the financial institution's ecosystem.

9.2.4. Financial institutions should ensure that cyber threat intelligence is made available to appropriate staff with responsibility for the mitigation of cyber risks at the strategic, tactical and operational levels within the financial institution. Cyber threat intelligence should be used to ensure that the implementation of any cyber resilience measures is threat-informed. When properly contextualised, cyber threat information enables a financial institution to validate and inform the prioritisation of resources, risk mitigation strategies and training programmes.

9.3. Information-sharing

9.3.1. To facilitate sector-wide response to large-scale incidents, financial institutions should plan for information-sharing through trusted channels in the event of an incident, collecting and exchanging timely information that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants during and following a cyber attack. Financial institutions should, as part of their response programmes, determine beforehand which types of information will be shared, with whom, and how information provided to the financial institution will be acted upon. Reporting requirements and capabilities should be consistent with information-sharing arrangements within the financial institution's communities and the financial sector. The financial institutions' incident reporting template is shown in Appendix A.

9.3.2. Financial institutions should participate actively in information-sharing groups and collectives, including cross-industry, cross-government and cross-border groups to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats. Financial institutions should, where appropriate, share information both bilaterally and multilaterally. As appropriate, a financial institution should consider exchanging information on its cyber resilience framework bilaterally with trusted stakeholders so as to promote understanding of each other's approach to securing systems that are linked or interfaced. Such information exchange would facilitate a financial institution's and its stakeholders' efforts at dovetailing their respective security measures to achieve greater cyber resilience. Multilateral information-sharing arrangements should be designed to facilitate a sector-wide response to large-scale incidents.

9.3.3. Central Bank shall set up and lead the following initiatives:

a. The Central Bank shall set up initiatives for sharing threat, vulnerability and mitigation information in the financial sector. Financial institutions are required to participate. All participants are expected to share information promptly, follow rules, use secure channels and maintain confidentiality.
b. The Central Bank shall also lead the establishment of a Computer Security Incident Response Team (CSIRT) for use by all participants in the financial sector. Financial institutions shall participate in both establishment and operation of the CSIRT.

10. Learning and evolving

10.1. Preamble

10.1.1. A financial institution's cyber resilience framework needs to achieve continuous cyber resilience amid a changing threat environment. To be effective in keeping pace with the rapid evolution of cyber threats, a financial institution should implement an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and allows the financial institution to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. A financial institution should aim to instill a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

10.2. Ongoing learning

10.2.1. A financial institution should systematically identify and distil key lessons from cyber events that have occurred within and outside the organisation in order to advance its resilience capabilities. Useful learning points can often be gleaned from successful cyber intrusions and near misses in terms of the methods used and vulnerabilities exploited by cyber attackers.

10.2.2. A financial institution should actively monitor technological developments and keep abreast of new cyber risk management processes that can effectively counter existing and newly developed forms of cyber attack. A financial institution should consider acquiring such technology and know-how to maintain its cyber resilience.

10.2.3. Financial institutions' cyber risk management practices should go beyond reactive controls and include proactive protection against future cyber events. Predictive capabilities and anticipation of future cyber events are based on analysing activity that deviates from the baseline. Financial institutions should work towards achieving predictive capabilities, capturing data from multiple internal and external sources, and defining a baseline for behavioural and system activity.

10.3. Cyber resilience benchmarking

10.3.1. Metrics and maturity models allow a financial institution to assess its cyber resilience maturity against a set of predefined criteria, typically its operational reliability objectives. This benchmarking requires a financial institution to analyse and correlate findings from audits, management reviews, incidents, near misses, tests and exercises

as well as external and internal intelligence gathered. The use of metrics can help a financial institution to identify gaps in its cyber resilience framework for remediation, and allow a financial institution to systematically evolve and achieve more mature states of cyber resilience.

11. Remedial measures and administrative sanctions

The Bank shall monitor financial institutions' compliance with these Guidelines. If a financial institution fails to comply with this Guidelines in a flagrant manner and which results, or threatens to result, in an unsafe or unsound operating condition, as determined by the Central Bank, the Central Bank will pursue any or all corrective actions and penalties as provided for under the Central Bank Order, 1974, the Financial Institutions Act, 2005, Exchange Control Order, 1974, and National Clearing and Settlement Systems Act, 2011 or any other relevant Acts or their successor legislation. Enforcement action by the Bank shall be timely, objective, firm, and may be publicized to increase awareness and promote consumer trust.

12. Enquiries

Any enquiries relating to this Guideline should be addressed to the General Manager, Financial Regulation Central Bank of Eswatini, P.O. Box 546, Mbabane or Telephone 2408 2148.

_____

Majozi V. Sithole
GOVERNOR, CENTRAL BANK OF ESWATINI

13. Appendix A

Cybersecurity Incident Notification Form			
Name Of Institution:			
Date: (dd/mm/yy)		**Time: (HH:MM)**	
Cyber Incident Prioritization			**Mark X**
High	The incident affects the whole organization. All or most of the institution's critical systems are affected		
Medium	The incident affects a section/division or multiple business units. It affects some part of the institution's operations		
Low	The incident affects an individual or a small group of people and has little or no impact on the institution's operations		
Description of Cyber Incident			
Title: XXXX		**Title: XXXX**	
Full Name		**Full Name**	
Signature		**Signature**	