Part A: Governance

Preamble

Governance refers to the decisions and actions of those in charge of an entity. More specifically, cyber resilience governance is concerned with the overall formation, execution, and evaluation of a cyber risk management approach.

Effective and efficient governance is key to the success of any business entity. Executed properly, it allows for rapid yet thorough decision-making and information dissemination, which are vital in a world where the cyber threat environment is ever-changing and evolving.

It is therefore ~~incumbent upon~~crucial that the board and senior management of ~~an entity to~~entities ensure ~~the adequate management of~~that they adequately manage cyber ~~risk~~risks. This includes overseeing the employment of a cyber resilience strategy and framework from conception to implementation, and reviewing this strategy and framework frequently to ensure its continuing effectiveness in the dynamic cyber threat environment. The cyber resilience strategy and framework can be standalone files or well embedded in an ~~entity's~~entities other ~~strategy~~strategies and ~~framework~~frameworks (e.g. IT security strategy/framework).

Clearly defined cybersecurity roles and responsibilities are integral to this process, not only to the framework itself but also to the fostering of a culture in which all staff understand their individual and collective importance in upholding an entity's cyber resilience.

Furthermore, due to the increasing interconnectedness of the financial sector, the ability to respond quickly and with accuracy can be instrumental in preventing the most catastrophic of cyberattack consequences, from loss of customer data, to complete systemic failure.

This section provides guidance on how entities should use good governance to appropriately manage the overall cyber risk to themselves, and by extension, the financial sector as a whole. The recommendations included in this section are all baseline recommendations, as good governance is vital to successful cyber risk management ~~and it~~. It is therefore imperative that all entities focus on building their governance to at least the baseline level.

Part A: Governance sets the foundation for a sound cyber risk management framework and is relevant to all other three parts of the guidance - Part B: Capability building, Part C: Information sharing and Part D: Third-party management. Entities should emphasise the overarching role of governance in each step of strengthening cyber resilience.

A1. Board and Senior Management Responsibilities

A1.1 The board should be ultimately responsible for the cyber resilience of an entity.

A1.2 The board should ensure that it understands the cyber risk environment faced by the entity. If necessary, the expertise required to understand the cyber risk could be accessed through other experienced in-house staff or external independent organisations.

A1.3 The board and senior management should assign a senior executive with the appropriate skills, knowledge and experience to be accountable for the cyber resilience strategy and framework.

A1.3.1 The board and senior management should ensure the appointed senior executive be able to directly report observance/issues of the cyber resilience of the entity to its senior management and the board.

A1.3.2 The appointed senior executive should not interfere with the entity's internal audit on the cyber risk management of the entity.

A1.4 The board and senior management should ensure that all staff with cyber resilience-related roles and responsibilities have the skills, knowledge, experience and resources to perform their required tasks effectively, and are informed and empowered to act in a timely manner.

A1.5 The board and senior management should be responsible for determining the entity's cyber risk tolerance and appetite, in order to oversee the formulation of a commensurate cyber resilience strategy and framework.

A1.6 The board should be responsible for approving the entity's cyber resilience strategy and framework, and monitoring the entity's implementation of the cyber resilience framework, including policies, procedures and controls that support the implementation.

A1.7 Senior management should regularly keep the board apprised of the cyber resilience status of the entity, including any changes to the entity's vulnerabilities or the cyber threat environment, in order to ensure continued consistency with the entity's cyber risk tolerance and appetite.

A1.7.1 Senior management should include in these board updates a plan for future resource allocation, including for both ongoing and forecasted cyber resilience needs.

~~A1.8.1 The board and senior management should ensure the appointed senior executive can act independently from the IT/operations department and be able to report to senior management and the Board directly.~~

~~A1.8.2 The appointed senior executive should not be involved in internal audit activities.~~

A2. Cyber Resilience Strategy and Framework

A2.1 The entity should develop a clear cyber resilience strategy and framework commensurate with its vulnerabilities and exposure to threats.

A2.1.1 The cyber resilience strategy should outline:

- The importance of cyber resilience to the entity;
- The entity's stakeholders' high-level requirements;
- The entity's vision and mission regarding cyber resilience;
- The entity's cyber resilience objectives;
- The entity's cyber risk appetite;
- The entity's cyber resilience targets and implementation plan;
- The high-level scope of technology and assets which will be used to manage cyber resilience;
- How cyber resilience initiatives will be delivered, managed and funded;
- The integration of cyber resilience with people, processes, technology, and new or existing business initiatives.

A2.1.2 The cyber resilience framework should:

- Set out how the entity sets its risk tolerance and cyber resilience objectives and how the entity identifies, mitigates and manages its cyber risk to support its objectives;
- Incorporate the recommendations of this guidance related to governance, capability building, information sharing and third-party management;
- Be designed using leading international and national standards and guidelines as a benchmark;
- Be consistent with the entity's risk management framework.

A2.2 The entity should ensure that its cyber resilience strategy and framework are aligned with its business objectives, stakeholder requirements, corporate strategy, risk management framework, and other related strategies and frameworks.

A2.3 The entity should ensure that its cyber resilience strategy and framework are commensurate with its risk tolerance and appetite.

A2.4 The entity should ensure that all cyber resilience-related roles and responsibilities are clearly defined within the cyber resilience framework, and are aligned with the cyber resilience strategy.

A2.5 The entity should have an internal audit process to help monitor and measure the implementation progress, adequacy and effectiveness of its cyber resilience strategy and framework. The entity should ensure the independence of its internal audit team either by using its in-house internal audit capability or external resources.

A2.6 The cyber resilience strategy and framework should be reviewed and updated regularly to ensure the entity can continue sound business operation amid any shifts in the cyber risk environment.

A3. Culture and Awareness

A3.1 The entity should promote a culture that recognises that staff at all levels have important responsibilities in ensuring its cyber resilience.

A3.1.1 This culture should be conveyed through clear and effective internal communication, and should include ~~the dissemination~~sharing relevant information of the cyber resilience strategy and framework to all staff.

A3.2 The entity should build and nurture a strong level of awareness of, and commitment to, cyber resilience business-wide.

A3.2.1 The entity should have a process for gathering, analysing ~~and disseminating~~ cyber threat intelligence as it emerges~~, in order~~ and share as appropriate with staff to aid in business-wide situational awareness.

A3.3 The entity should develop and maintain a programme for continuing cyber resilience training for staff at all levels, including the board and senior management, throughout each phase of the employment lifecycle (in other words, recruitment, on-boarding, training and development, and off-boarding) and in line with recognised industry standards for cybersecurity.

A3.3.1 The training should include current cyber threats, attack tactics, and appropriate incident responses.

A3.3.2 The frequency and content of the training should be adjusted according to respective roles and responsibilities, and any additional account permissions or security access the employee might have.

Part B: Capability Building

Preamble

Capability building encompasses five technical building blocks that form the foundation for robust cyber resilience. These building blocks allow an entity to identify, protect against, detect, respond to, and recover from, cyber threats and incidents.

Identification and classification of critical functions ensures that an entity can more effectively prioritise and protect its most important information assets and operations against potential cyber threats. Additionally, an entity's ability to understand both its internal situation and its external responsibilities to the stability of the wider financial sector is vital in ensuring it efficiently responds to and recovers from cyber incidents.

Furthermore, protecting an entity's critical functions means safeguarding the confidentiality, integrity and availability of its information assets and operations. The security controls implemented to do so should be commensurate with an entity's cyber risk tolerance as well as the continual changes in its cyber threat environment.

Cyberattacks are increasing in frequency and sophistication, and are generally stealthy in their execution. Therefore, possessing the capability to spot the signs of an impending cyber incident and detect a breach is vital to an entity's cyber resilience. Early warning allows an entity the time to defend against or contain a potential breach, effectively mitigating the negative impact the cyber incident otherwise might have had.

Response and recovery plans are essential to an entity's ability to return to business as usual when a cyber incident has occurred. As a result, these plans are also fundamental in ensuring continued stability of the financial system as a whole. It is therefore incumbent upon an entity to have arrangements in place to resume critical functions as quickly and accurately as can be safely achieved. Post-incident analysis is important in understanding learnings from cyber incidents and integrating them back into the response and recovery plans.

Testing is another integral part of developing strong cyber resilience, whether it be penetration testing, vulnerability assessments, or business impact analyses. All elements of an entity's cyber resilience framework should be regularly tested and updated, in order to remain effective against ever-evolving cyber risk.

This section of the guidance follows the structure of the NIST's Framework for Improving Critical Infrastructure Cybersecurity and outlines how an entity should utilise, and improve where necessary, their identification, protection, detection, response and recovery capabilities to lay the foundation for building robust cyber resilience.

B1. Identify

Baseline:

B1.1 The entity should identify, classify according to criticality and sensitivity, record, and regularly update all of its critical functions, including the information assets, key personnel roles, and processes that support these functions. This will enable the entity to prioritise the processes of protection, detection, response and recover for each of these functions.

B1.2 The entity should also create and maintain an up-to-date inventory of all individual and system accounts, taking care to include those with remote access or privileged access rights, in order to ensure access to sensitive information and supporting systems is kept on an as-needed basis only.

B1.3 The entity should create and regularly update a map of its network resources, including IPs, devices, servers, and any external network links that support the entity's critical functions.

B1.4 The entity should make sure these identification and classification efforts are integrated with other relevant processes, such as acquisition and change management, in order to ensure inventories are kept up-to-date, as well as remaining both accurate and complete.

B1.4.1 Cyber risk assessments should be conducted before new or updated technologies, products, services or processes are introduced, in order to identify any associated threats or vulnerabilities.

Enhanced:

B1.5 The entity should carry out a holistic self-assessment risk assessments on a regular basis in order to identify new vulnerabilities and cyber threats as they emerge, and feed these issues and mitigating actions back into the cyber resilience strategy and framework.

B2. Protect

Baseline:

B2.1 The entity should have security controls in place, based on the identified critical functions, which allow it to achieve its security objectives and meet business requirements while minimising the probability and potential impact of a cyberattack.

B2.1.1 The entity's security objectives should include ensuring the continuity and availability of its information systems as well as protection of the integrity, confidentiality and availability of data and information while stored, in use or in transit.

B2.1.2 The entity should regularly update its security controls should be regularly updated to ensure they the approaches it adopts remain commensurate to the entity's critical functions, cyber threat landscape and systemic importance.

~~B2.2 The entity should segment its network infrastructure with security controls appropriate to its design principles and commensurate to its risk profile.~~

B2.3 The entity should regularly monitor its systems throughout its life cycle, in order to identify weaknesses~~, and~~. It should also ensure all available updates are installed and sufficient support is maintained~~.~~, as appropriate.

B2.3.1 Additional layers of security should be implemented and tested where vulnerabilities are identified in systems.

B2.3.2 Legacy systems that are outdated, have limited or no support, or have vulnerabilities that cannot be adequately patched or mitigated through segregation from other systems, should be decommissioned and replaced.

B2.4 The entity should ensure that access to systems and information is controlled so that only staff who are authorised to access them can do so.

B2.4.1 Authorisation should be restricted according to the principle of least privilege, meaning granting the bare minimum access only to those who have a legitimate business reason for it, and are trained to use the system or information appropriately.

B2.4.2 The entity should have controls in place that strictly limit and monitor staff with greater/privileged access entitlements.

B2.4.3 The entity should have processes in place to monitor system and information access and trigger an alert when unauthorised access is attempted or granted.

B2.4.4 The entity should have processes in place to monitor employees changing roles or leaving the entity, to ensure all access rights are updated accordingly when the change takes place.

B2.5 The entity should have policies, procedures and controls in place for change management and ensure cyber security is considered throughout the life ~~cyber~~cycle of the change management process.

B2.6 The entity should implement screening and background checks for all new employees and contractors before they are hired/contracted ~~as well as for existing employees on a regular basis, proportionate to their access rights~~. When an employee is changing responsibilities, the entity should ensure that all access rights that are related to the employee's previous position and are not necessary for the employee's new responsibilities are revoked in due time. Employees in sensitive positions (e.g. those who change to roles requiring privileged access to critical systems or who become high-risk staff) should be pre-screened.

B2.7 The entity should have strong controls in place to identify and prevent data loss through removal from the entity's systems.

Enhanced:

B2.8 The entity should adopt a 'resilience by design' approach to designing its systems, processes, products and services. This means embedding the resilience measures within the systems, processes, products and services from the first stage of design and development.

B2.9 The entity ~~should~~could find it useful to implement automated mechanisms that can isolate affected information assets in the case of an adverse event as appropriate.

B3. Detect

Baseline~~:~~

B3.1 The entity should document the normal baseline performance for its identified critical functions and supporting systems, so that any deviation from the baseline can be detected and anomalous activities and events can be flagged for investigation.

B3.1.1 The entity should ensure that it has the right capabilities in terms of people, processes and technologies in place to monitor and detect deviations from normal system activity.

B3.1.2 The entity should have criteria in place to trigger alerts when anomalous activities occur. This should also include thresholds for triggering a cyber incident alert and response process.

B3.1.3 The entity should ensure that these detection and monitoring capabilities, as well as the system performance baselines, trigger criteria, and alerts are reviewed, tested and updated regularly to ensure accuracy in cyber risk screening and remain commensurate with the entity's cyber threat environment.

B3.2 The entity should define alert threshold for its monitoring and detection systems in order to trigger and facilitate its incident response plan.

B3.3 The entity should ensure that the relevant staff are trained to be able to identify and report anomalous activities, events and incidents; this training should be updated regularly to be commensurate with any changes to the entity's cyber threat environment.

B3.4 The entity should incorporate multiple layers in its detection controls, including people, processes and technology; these controls should have the capability to detect cyberattacks and isolate the point of corruption.

B3.5 The entity should ensure that its detection and monitoring capabilities allow for sufficient information collection to support forensic investigation of events and incidents.

B3.5.1 Information, system and data logs should be backed up to a secure location and have controls in place to ensure the logs remain accurate, uncompromised, and free from interference.

B3.6 The entity should ensure analysis of the information collected from the monitoring of systems and user activity is carried out in a timely manner; this analysis should be used to enhance its detection capabilities, tactics, and incident response process.

~~**Enhanced:**~~

B3.7 The entity should conduct ~~penetration~~security tests on their systems and networks to detect weaknesses that could be exploited by a cyberattack or leave them exposed to a cyber incident.

B3.7.1 The ~~penetration~~ tests should be conducted on a regular basis, as well as each time a major change occurs to the cyber threat status of the entity, such as when the entity implements new systems or technologies.

B3.7.2 The ~~penetration~~ tests should involve, if deemed necessary, all relevant internal staff and departments that are critical to the cyber resilience of the entity and relevant third parties.

B4. Respond and Recover

Baseline:

B4.1 The entity should have response and recovery plans in place for when a cyber incident or breach occurs.

B4.1.1 These plans should be based on the aforementioned identification and categorisation of its critical functions, and include operating in a diminished capacity; safe restoration of systems and services in the order of their relative priority; recovery point objectives; and recovery time objectives, commensurate to the entity's requirements and its systemic importance.

B4.1.2 These plans should work to avoid or limit as much damage as possible following a cyber incident or breach, while also reducing recovery time and costs.

B4.1.3 These plans should outline the internal and external stakeholders that must be notified of a cyber incident, when a notification must occur, and what information needs to be included in the notification. The level of stakeholder engagement should be informed by the severity and impact of a cyber incident.

B4.1.4 These plans should also outline the criteria for escalation within the entity, including to senior management and the board, based on the potential impact of the cyber incident.

B4.1.5 These plans 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 entity.

B4.1.6 The entity should contemplate a wide range of different cyber incident scenarios when formulating the response and recovery plans, and in doing so conduct business impact analyses to assess how each scenario would impact the entity so that it can respond accordingly. These impact analyses should be conducted regularly and updated to reflect the ever-evolving cyber threat landscape that the entity faces.

B4.2 The entity's cyber incident response and recovery plans should be aligned with its business continuity plan, as well as any other relevant plans.

B4.3 The entity should ensure that the staff responsible for responding to cyber incidents and breaches have the required skills and training to address the situation appropriately.

B4.4 The entity should utilise its process for triggering cyber incident alerts, outlined under 'Detect', to ensure the right staff are aware of the incident or breach and have the most up-to-date information so that they can respond accordingly.

B4.5 The entity should regularly review and test its response and recovery plans, using a range of different scenarios, to ensure their continued effectiveness.

B4.6 The entity should have processes in place that enable it to collate and review information from cyber incidents and testing results, so that it can constantly improve its response and recovery plans to be commensurate with the ever-evolving cyber risk environment.

B4.7 The entity should have processes and procedures in place to conduct ~~an ex post~~post-incident analyses to identify root ~~cause analysis~~causes of its cybersecurity incidents, and integrate its findings back into its response and recovery plans.

Enhanced~~:~~

B4.8 The entity should consult with relevant external stakeholders (regulators, cybersecurity agencies, other entities in the financial sector) to develop common response and recovery plans for cyber incidents that may affect the financial sector.

B4.8.1 The entity, together with ~~the other~~relevant external stakeholders, should conduct regular testing of the common response and recovery plans, in order to gauge the impact of a wide range of cyber scenarios on the financial sector as a whole, as well as the stakeholders' collective ability to respond and recover adequately to such scenarios.

Part C: Information sharing

Preamble

Facing ever-evolving and ~~highly~~ contagious cyber threats, the benefits of collective action are apparent. A crucial component of a collective response to cyber threats is the sharing of information and how quickly it can be acted upon. In addition to the cyber threat environment, it is also crucial for an entity to understand the adequacy of its cyber risk mitigation measures through sharing and learning from industry best practice.

Information that can be shared includes, but is not limited to, indicators of compromise (IOC), cyber incidents, threats, vulnerabilities, risk mitigation, best practice and strategic analysis. Sufficiently detailed anonymised data shared on appropriate platforms help entities to react quickly and appropriately to cyber threats. It is encouraged and considered prudent to participate in cybersecurity information exchange groups (for example, ~~FSIE~~Financial Sector Security Information Exchange, organised by NCSC) and collaborate with trusted stakeholders within and outside of the industry.

Entities should also meet all regulatory requirements regarding reporting and sharing information on cyber resilience.

This section of the guidance outlines how an entity should make preparations for sharing information through trusted channels and have a process in place to ensure the sharing is safe and timely, to promote the cyber resilience of the entity and the financial system.

C1. Channels

Baseline~~:~~

C1.1 The entity should plan for information sharing through trusted channels: collecting and exchanging timely information that could facilitate the detection, response and recovery of its systems from cyber incidents.

C1.2 The entity should meet relevant regulatory requirements for reporting information regarding cyber incidents and cyber resilience preparedness.

C1.3 The entity ~~could~~would find it helpful to participate in information sharing groups and collectives to gather, distribute and assess information about cyber practices, cyber risk, and early warning indicators relating to cyber threats.

C2. Process

Baseline:

C2.1 The entity should determine beforehand which types of information will be shared, the circumstances under which sharing is permitted, with whom the information can and should be shared, and how the information provided to the entity should be acted upon.

C2.2 The entity should have in place a process that enables it to access and share information with external stakeholders (for example, regulators and cybersecurity agencies) in a timely manner, as well as meet regulatory reporting timeframes, if required. The process for information sharing, especially contact information, should be maintained and updated regularly.

Enhanced:

C2.3 The entity ~~could~~would find it helpful to adopt the Traffic Light Protocol to ensure that sensitive information is shared with the correct audience.

C2.4 The entity ~~could~~would find it helpful to develop models to estimate and capture financial losses from cyber incidents, not only for the purpose of information sharing, but also to improve overall cyber risk management.

Part D: Third-party management

Preamble~~:~~

It has become the norm for organisations ~~today~~ to rely on a multitude of third-party service providers (including related parties, like parent companies or subsidiaries) to support core business functions. It is also common for these third-party entities to have access to a company's data and its internal systems. ~~The~~If used prudently, third-party services may reduce an entity's cyber risk, especially for those entities that lack cyber expertise. However, the third-party ecosystem provides an ideal environment for cyber criminals looking to infiltrate an organisation to thrive. ~~Additionally, cyber risk grows as these networks become larger and more complex.~~

Extensive use of third-party services increases the difficulty of assessing an entity's level of cyber resilience and exposure to cyber risk, both for the entity itself and its regulators. In addition, third parties increasingly rely on other service providers, therefore introducing additional vulnerabilities and threats.

An entity's board of directors and senior management bear the ultimate responsibility to ensure its outsourced service is performed safely and soundly. The entity should be fully aware of the cyber risk associated with third parties and act appropriately to mitigate that risk. The entity should integrate cyber resilience when developing and updating its outsourcing framework.

Besides the cyber risk associated with outsourcing, entities should also pay attention to the cyber risk arising from the interconnectedness of the financial ecosystem.

This section of the guidance outlines how an entity should plan, screen, review, and use contracts to manage its relationship with third-party service providers, while also undertaking ongoing cyber risk management to ensure cyber risks arising from third parties are under control.

This section also provides high-level recommendations regarding the use of third-party cloud computing service providers. ~~Migrating~~If managed prudently, migrating to the cloud ~~may present~~presents a number of benefits including geographically dispersed infrastructures, agility to scale more quickly, improved automation, sufficient redundancy, and reduced initial investment ~~cost~~costs for individual financial institutions. However, using cloud services ~~does bring more~~brings challenges to assess legal and regulatory obligations and financial institutions may also run the risk of potentially ~~underinvest~~underinvesting in risk mitigation if the shared tasks are not well articulated and understood.

~~*Where an entity is required to comply with the Outsourcing Policy (BS11), it should read this guidance in conjunction with BS11. For those detailed requirements not specified in this guidance, for example the frequency of conducting response testing and the format of the inventory of outsourced arrangements, an entity must refer to*~~

The trend of relying on a narrow set of major cloud service providers also puts concentration risks on the financial system. Therefore, in addition to following all recommendations on general third-party management, financial institutions should pay special attention when outsourcing to cloud service providers.

D1. Planning

Baseline:

D1.1 The entity should assess the criticality and sensitivity of the activities/data/processes being outsourced before entering into any outsourcing contracts.

D2. Due diligence

Baseline:

D2.1 The entity should perform due diligence and document the due diligence results before signing any contracts, in order to evaluate the third parties' ability to meet the cyber resilience specification of the entity.

Enhanced:

D2.2 The entity could find it helpful to use a standard assessment questionnaire when doing its due diligence or develop a custom questionnaire according to the entity's risk appetite and its business requirement.

D2.3 The entity could find it useful, when doing its due diligence, to obtain independent security attestation reports and certifications as a means to provide assurance as to the security posture of its third party service provider.

D3. Contract negotiation

Baseline:

D3.1 The entity should use contracts with third parties to ~~clearly specify~~capture cyber security considerations that are commensurate with the ~~cybersecurity-related~~entity's cyber risk appetite. This may include roles and responsibilities ~~(for example,~~of each involved party regarding data access, incident response and communication, business continuity ~~plan~~planing, termination, and data portability, etcetera~~.) for each party involved~~.

Enhanced:

D3.2 The entity could find it useful to be fully informed about any related subcontracting by third parties that the entity has an outsourcing arrangement with. An entity could agree to allow a third-party to subcontract only when the subcontractors can fully meet the obligations existing between the entity and their outsourcing service providers.

D3.3 The entity may find it helpful to consider portability and interoperability of their data and applications and include provisions in its outsourcing contracts to avoid vendor lock-in.

D4. Ongoing cyber risk management

Baseline:

D4.1 The entity should consider the cyber risk associated with its third parties in each stage of its own capability building described in Part B. The entity should:

D4.1.1 Clearly identify and document the cyber risk associated with using third ~~parties~~-party service providers and update this information on a regular basis.

D4.1.2 Design and verify security controls to detect and prevent intrusions from third-party connections.

D4.1.3 Ensure that third-party employee access to the entity's confidential data is tracked actively, based on the principle of least privilege.

D4.1.4 Integrate third parties that provide services for the entity's critical functions into the entity's response plan ~~and involve them in response testing~~.

D4.2 The entity should assess the substitutability of the third parties that provide services for the entity's critical functions, and ~~prepare for~~include transitioning to alternative service providers or performing critical services in-house in its business continuity plan that is commensurate with the criticality of the services and the entity's risk appetite.

Enhanced

D4.3 The entity could find it useful to conduct response and recovery testing with its third-party service providers and use the testing results to improve its response and recovery plans.

D5. Review and accountability

Baseline:

D5.1 The entity should regularly assess its third-party service providers' cybersecurity capabilities at least. The assessment can be achieved through the services providers' self-assessment if not through conducting its , the entity's own assessment, or assessment by independent third parties.

Enhanced

~~**Enhanced:**~~

D5.2 The entity could find it useful to obtain assurance of its third-party service providers' cyber resilience capabilities by using tools such as certifications, external audits, summary of test reports, etcetera.

D6. Documentation

Baseline:

D6.1 The entity should maintain an up-to-date, comprehensive inventory of its third-party service providers and interconnection with other entities, as well as regularly updating the networking map of its external dependencies.

D7. Termination

Baseline:

D7.1 The entity should establish a termination/exit strategy for the third parties that provide services related to the critical functions of the entity.

D8. Outsourcing to Cloud Service Providers

Baseline:

D8.1 The entity should inform the Reserve Bank about their outsourcing of critical functions to cloud service providers early in their decision-making process.

D8.2 The entity should evaluate and have a clear understanding of the rationale and the potential impacts of outsourcing to cloud service providers.

D8.3 The entity should know in which be aware of the jurisdiction the cloud service provider's business premises are located and where theirrisk associated with data will be stored,

processed and transmitted in the cloud, including data replicated for provision of backup or availability services. The entity should assess the potential legal risk, compliance issues and oversight limitations associated with ~~the location(s) of its outsourced~~outsourcing to cloud service providers.

D8.4 The entity should carefully consider the different levels of roles and responsibilities when entering into an agreement with its cloud service provider using the shared responsibility model. The entity may refer to NCSC's ~~high-level~~high-level guidance on the shared responsibility model.

D8.5 The entity should consider and make it clear in the outsourcing agreement about how data will be segregated if using a public cloud service provider.

Enhanced~~:~~

D8.6 ~~The entity may find it helpful to consider portability and interoperability of their data and applications, and include provisions in its outsourcing contracts to avoid vendor lock-in, should they wish to move to a different cloud service provider in future.~~

~~D8.7~~ The entity may find it helpful, when ~~taking~~conducting its own due diligence, to take account of the cloud service provider's adherence to international standards as relevant.

D8.~~8~~7 The assessment of the design and operating effectiveness of controls within the shared responsibility model (for both provider and the entity itself) should be commensurate with the impact of the outsourced functions/systems on the entity.

Annexes

Glossary

This guidance uses the “Cyber Lexicon” developed by the Financial Stability Board (2018) as the main reference for the glossary. The “Cyber Lexicon” draws on extensive work that has previously been done by international groups, such as the work of CPMI-IOSC in its guidance on cyber resilience for financial market infrastructures, the work of NIST in its glossary of key information security terms, and the work of ISO. For certain terms not covered by the “Cyber Lexicon”, NIST is used as the ultimate reference for this glossary. The glossary focuses on the core terms necessary to support the objective of this guidance.

Availability	Property of being accessible and usable on demand by an authorised entity.
Business continuity plan	The documentation of a predetermined set of instructions or procedures that describe how an entity’s business processes will be sustained during and after a significant disruption.
Business impact analysis	An analysis of an information system’s requirements, functions, and interdependencies used to characterise system contingency requirements and priorities in the event of a significant disruption.
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems.
Critical function	Any activity, function, process, or service, the loss of which (for even a short period of time) would materially affect the continued operation of an entity, the market it serves and the broader financial system, and/or materially affect the data integrity, reputation of an entity and confidence in the financial system.
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.
Cyber attack	The use of an exploit by an adversary to take advantage of a weakness with the intention of achieving an adverse effect on the ICT environment of an entity.
Cyber event	Any observable occurrence in an information system. Cyber events sometimes provide an indication that a cyber incident is occurring.

Cyber governance	Arrangements an organisation puts in place to establish, implement and review its approach to managing cyber risk.
Cyber incident	A cyber event that: i. jeopardises the cybersecurity of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
Cyber incident response plan	The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber incident.
Cyber resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.
Cyber resilience framework	Consists of the policies, procedures and controls an entity has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces.
Cyber resilience strategy	An entity's high-level principles and medium-term plans to achieve its objective of managing cyber risk.
Cyber risk	The combination of the probability of cyber incidents occurring and their impact.
Cyber risk management	The process used by an entity 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.
Cyber risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Cyber risk appetite	The level of tolerance that an entity has for cyber risk. It includes how much cyber risk an entity is willing to tolerate and how much an entity is willing to invest or spend to manage the risk.

Cybersecurity	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium.
Cyber threat	A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity.
~~Defence-in-depth~~	~~Security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation.~~
Information sharing	The exchange of data, information and/or knowledge that can be used to manage risks or respond to events.
Information asset	Any piece of data, device or other component of the environment that supports information-related activities.
Integrity	Property of accuracy and completeness.
Least privilege	The principle that the security architecture should be designed so that each entity is granted the minimum system resources and authorisations that the entity needs to perform its function.
Penetration testing	A method of testing in which assessors, using all available documentation (for example, system design, source code, manuals, etcetera.) and working under specific constraints, attempt to circumvent the security features of an information system.
Recovery point objective	The point in time to which data must be recovered after an outage.
Recovery time objective	The period of time, following a cyber incident, within which a function needs to resume or resources need to be recovered.
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.
System development life cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.

Third party	A person that is not the entity, including any related parties of the entity, for example, its parent companies or subsidiaries.
Threat intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes.
Traffic Light Protocol	A set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours to indicate expected sharing boundaries to be applied by the recipient(s).
Vulnerability	A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats.

Acronyms

CERT NZ	Computer Emergency Response Team New Zealand
CPMI-IOSC	Committee on Payments and Market Infrastructures – International Organization of Securities Commissions
CSA	Cyber Security Associates
FSIE	~~Financial Services~~Finance Security Information Exchange
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NZISM	New Zealand Informational Security Manual

Recommended frameworks for entities to refer to

GCSB (Government Communications Security Bureau) New Zealand Information Security Manual (NZISM)

NIST (National Institute of Standards and Technology) Cybersecurity Framework

Cyber Risk Institute Cybersecurity Profile (previously known as Financial Services Sector Cybersecurity Profile)

ISO/IEC 27000-series of information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)