Information Technology Risk Management Guidance

(VER01.201124)

TABLE OF CONTENTS

Introduction 1
Background 1
Structure of the Guidance 2
Applicability 7
Building Effective Control Environments 8
Section A: Establishing a Culture of Effective IT Risk Management 10
Chapter 1 – Governance and Oversight 10
Desired Outcome 1.1 – Strategy Alignment 10
Desired Outcome 1.2 – Competence 10
Desired Outcome 1.3 – Accountability 11
Chapter 2 – Risk Management 13
Desired Outcome 2.1 – Risk Awareness 13
Desired Outcome 2.2 – Risk Awareness Training 14
Desired Outcome 2.3 –Risk Assessment Framework 15
Desired Outcome 2.4 – Risk Monitoring 18
Desired Outcome 2.5 – Incident Management 19
Desired Outcome 2.6 – Problem Management 22
Desired Outcome 2.7 – Insider Risk 22
Chapter 3 – Third Party Management 23
Desired Outcome 3.1 – Third Party Risk Governance 23
Desired Outcome 3.2 – IT Third Party Lifecycle Management 25
Desired Outcome 3.3 – Supply Chain Resilience 28
Chapter 4 – Compliance and Audit 30
Desired Outcome 4.1 – Comply 30
Desired Outcome 4.2 – Audit 30
Section B: Managing an IT Environment 32
Chapter 5 – System Lifecycle Management 32
Desired Outcome 5.1 – Project Management Oversight 32
Desired Outcome 5.2 – System Acquisition, Development and Testing 33
Desired Outcome 5.3 – System Refresh and Decommissioning 37
Chapter 6 –Technology Asset Management 39
Desired Outcome 6.1 – Asset Identification and Classification 39
Desired Outcome 6.2 – Asset Accountability 40
Chapter 7 – Operational Infrastructure Management 41

Desired Outcome 7.1 – Standardising the Operating Environment 41
Desired Outcome 7.2 – Securing the Physical Environment 42
Desired Outcome 7.3 – Securing Connections 43
Desired Outcome 7.4 – Securing the Virtual Environment 48
Desired Outcome 7.5 – Updating the Environment 49
Chapter 8 – Data Lifecycle Management 53
Desired Outcome 8.1 – Data Governance 53
Desired Outcome 8.2 – Data Lifecycle Management 53
Desired Outcome 8.3 – Handling Data with Regulatory Obligations 57
Chapter 9 – Resilience 58
Desired Outcome 9.1 – Availability Architecture 58
Desired Outcome 9.2 – Continuity Planning 60
Desired Outcome 9.3 – Recovery Planning and Testing 61
Chapter 10 – Cyber Event Management 63
Desired Outcome 10.1 – Threat Awareness 63
Desired Outcome 10.2 – Cyber Event Lifecycle Management 64
Desired Outcome 10.3 – Security Testing 65
Section C: Interacting Securely 67
Chapter 11 – Access Management 67
Desired Outcome 11.1 – Credential Management 67
Desired Outcome 11.2 – Authorisation 69
Desired Outcome 11.3 – Authentication 70
Chapter 12 – Online Transaction Security 74
Desired Outcome 12.1 – Online Transaction Security 74
Desired Outcome 12.2 – Fraud Mitigation 75
Desired Outcome 12.3 – Customer IT Risk Awareness 76
Chapter 13 – Cryptography 77
Desired Outcome 13.1 – Cryptographic Schemes 77
Desired Outcome 13.2 – Key Lifecycle Management 78
Section D: Leveraging Business Embedded Technologies 80
Chapter 14 – Algorithm Driven Solutions 80
Desired Outcome 14.1 – Governance of Algorithm Driven Solutions 80
Desired Outcome 14.2 – Safe Development and Usage 82
Chapter 15 – Decentralised Infrastructure Solutions 84

Desired Outcome 15.1 – Understanding Decentralised Infrastructure Solutions 84

Desired Outcome 15.2 – Secure Participation 85

Annex A: Related ADGM Rules, Regulations and Guidance 88

INTRODUCTION

Background

i. Technology[1] and data are core enablers for modern financial institutions. Financial institutions rely on technology to conduct their operations, achieve business outcomes and serve their customers. They need data to support decision-making processes on all matters, including for operations and service delivery. Leveraging on technology and data has allowed modern financial institutions to provide increasingly effective and efficient services to their customers.

ii. Authorised Persons in the Abu Dhabi Global Market ("ADGM") are expected to adequately manage risks arising from the use of information technology for its business operations and services to customers. Sections 3.3.1(1) and 3.3.4 of the General Rulebook ("GEN") require Authorised Persons to establish and maintain risk management systems and controls to enable it to identify, assess, mitigate, control, and monitor its risks, and ensure that its affairs are managed effectively and responsibly by its senior management.

iii. The objective of this Information Technology Risk Management Guidance ("Guidance") is to provide Authorised Persons and Recognised Bodies (collectively referred to as 'financial institutions' in this Guidance) with a set of desired outcomes and best practices on the sound management of information technology risks. While this Guidance does not set out legally binding requirements, financial institutions should be cognisant of other existing regulations, rules and guidance issued by the Financial Services Regulatory Authority ("FSRA"), the Registration Authority, and the Office of Data Protection (collectively referred to as the 'Relevant ADGM Authorities') relating to the management of information technology[2].

iv. In formulating this document, the FSRA has taken reference from guidance on related matters set out by various international standard setting bodies and financial regulatory authorities, as well as leading industry standards on information technology and security.

v. In developing this Guidance, the FSRA had regard to the following considerations:

   a. Technological evolution – New risks will continue to arise as technology evolves. As such, it is not possible to exhaustively provide guidance for all potential scenarios. The FSRA has therefore taken a principles-based approach to provide flexible Guidance that can address existing risks and remain relevant for new risks. In addition to these principles, the FSRA has listed best practices that financial institutions should consider when following the principles and will update these practices over time.

   b. Interrelated risks – IT risks are closely related to and can heighten risks to financial institutions' operations and business models. The FSRA therefore encourages

[1] 'Technology' and 'Information Technology (IT)' are used interchangeably at various points in this Guidance.
[2] Refer to Annex A for a list of rules and guidance relating to information technology issued by the Relevant ADGM Authorities.

financial institutions to take a holistic risk management approach towards managing IT risks in relation to other risk types.

c. Proportionality – Financial institutions' size and capabilities can vary significantly depending on their operations and business models. The FSRA expects financial institutions to take a risk-based approach in dealing with IT risk that is proportionate and reflects the nature, scale and complexity of their business.

vi. Financial institutions should understand the types of risks that arise when the confidentiality, integrity or availability of IT is compromised. The following are key risks that should be well understood and effectively managed.

a. Risk of unauthorised access: This may be perpetrated by internal actors (insiders, disgruntled staff, etc.) or external actors (hackers, cyber criminals, etc.). Such threat actors may exploit unauthorised access to perform activities that benefit them or cause undesirable outcomes for the organisation.

b. Risk of data leakage or compromise: Threat actors may alter data within an organisation's systems or expose exfiltrated corporate or client data on the internet, causing harm to the organisation's reputation or adversely impacting clients. Such incidents may also result from the negligence of staff or authorised third parties.

c. Risk of system disruption: System disruptions can arise from malicious actions performed by threat actors, unintentional detrimental system or data modifications, or from software and hardware failures.

d. Risk of technology or service exploitation: Upon gaining unauthorised access, threat actors may exploit an organisation's technology resources for criminal gain at the organisation's expense (e.g., botnet crypto mining, etc.). Threat actors may even abuse an organisation's digital services to disrupt another organisation's systems (e.g., denial of service attacks) or to defraud an organisation's customers (e.g., financial scams).

Structure of the Guidance

vii. The Guidance comprises four sections, each with multiple chapters.

a. Section A: Establishing a Culture of Effective IT Risk Management: These chapters set out expectations for overall governance and controls for IT risk, including incident management, audit, and the management of IT third parties.

b. Section B: Managing an IT Environment: These chapters set out expectations for how financial institutions should manage IT assets, infrastructure, systems lifecycle, resilience, and cyber events.

c. Section C: Interacting Securely: These chapters set out expectations for how financial institutions should manage access to their systems, cryptographic keys and secure online transaction services.

d. Section D: Leveraging Business Embedded Technologies: These chapters set out expectations for how financial institutions should address the IT risks associated with specific technologies such as the use of algorithm-driven solutions (e.g., generative artificial intelligence models) and decentralised-infrastructure solutions (e.g., virtual assets platforms).

Sections	Chapters	Number of Desired Outcomes
A. Establishing a Culture of Effective IT Risk Management	1. Governance and Oversight 2. Risk Management 3. Third Party Management 4. Compliance and Audit	15
B. Managing an IT Environment	5. System Lifecycle Management 6. Technology Asset Management 7. Operational Infrastructure Management 8. Data Lifecycle Management 9. Resilience 10. Cyber Event Management	19
C. Interacting Securely	11. Access Management 12. Online Transaction Security 13. Cryptography	8
D. Leveraging Business Embedded Technologies	14. Algorithm-Driven Solutions 15. Decentralised Infrastructure Solutions	4

viii. Each chapter of the Guidance begins with desired outcomes that summarise the FSRA's expectations for financial institutions. For each of these desired outcomes, the FSRA has also set out specific best practices for financial institutions. For example, desired outcome 3.2 of the Guidance states that a financial institution should closely monitor and review its IT third parties' performance and risk posture. This is followed by specific best practices on conducting due diligence, developing contractual agreements, monitoring the performance of IT third parties and putting termination arrangements in place.

Section A: Establishing a Culture of Effective IT Risk Management

Chapter 1 – Governance and Oversight

Desired Outcome 1.1 – Strategy Alignment: A financial institution should ensure that its IT strategies are aligned with and support its overall business strategy.

Desired Outcome 1.2 – Competence: The Governing Body and senior management of a financial institution should ensure that its staff, and any third parties, are competent to perform their roles.

Desired Outcome 1.3 – Accountability: A financial institution should ensure that the appropriate staff are accountable for the management of IT risks.

Chapter 2 – Risk Management

Desired Outcome 2.1 – Risk Awareness: The Governing Body and senior management of a financial institution should foster a culture of IT risk awareness throughout the organisation.

Desired Outcome 2.2 – Risk Awareness Training: A financial institution should train its staff appropriately to mitigate IT risks.

Desired Outcome 2.3 –Risk Assessment Framework: A financial institution should put in place a risk assessment framework that identifies and assesses IT risks, and implements controls commensurate with the severity of the risks.

Desired Outcome 2.4 – Risk Monitoring: A financial institution should put in place a process to regularly monitor risk sources to ensure that the risk controls are functioning as designed.

Desired Outcome 2.5 – Incident Management: A financial institution should put in place procedures to detect, respond to and recover from incidents.

Desired Outcome 2.6 – Problem Management: A financial institution should establish a practice of studying past incidents and performance issues in a holistic manner to reduce the likelihood of future occurrences.

Desired Outcome 2.7 – Insider Risk: A financial institution should take steps to mitigate against insider threats.

Chapter 3 – Third Party Management

Desired Outcome 3.1 – Third Party Risk Governance: A financial institution should ensure that its engagement with third parties aligns with its business strategy and adheres to the established risk management framework.

Desired Outcome 3.2 – Third Party Lifecycle Management: A financial institution should closely monitor and review its third parties' performance and risk posture.

Desired Outcome 3.3 – Supply Chain Resilience: A financial institution should actively monitor and mitigate risks arising from its third parties' supply chain.

Chapter 4 – Compliance and Audit

Desired Outcome 4.1 – Comply: A financial institution should include IT obligations in its compliance programme.

Desired Outcome 4.2 – Audit: A financial institution should include IT controls in its audit programme.

Section B: Managing an IT Environment

Chapter 5 – System Lifecycle Management

Desired Outcome 5.1 – Project Management Oversight: A financial institution should ensure that IT projects align with its business strategy and adheres to the established risk management framework.

Desired Outcome 5.2 – System Acquisition, Development, and Testing: A financial institution should put in place a robust framework for managing the acquisition, development, and testing of systems.

Desired Outcome 5.3 – System Refresh and Decommissioning: A financial institution should establish processes to manage the safe and secure refresh and decommissioning of its systems.

Chapter 6 –Technology Asset Management

Desired Outcome 6.1 – Asset Identification and Classification: A financial institution should know what assets it has and how critical those assets are.

Desired Outcome 6.2 – Asset Accountability: A financial institution's assets should be responsibly managed in a way that is commensurate with the criticality of the assets.

Chapter 7 – Operational Infrastructure Management

Desired Outcome 7.1 – Standardising the Operating Environment: A financial institution should maintain an up-to-date library of standardised configurations that all hardware and software comply with.

Desired Outcome 7.2 – Securing the Physical Environment: A financial institution should ensure that all physical assets connecting to its networks are secured to prevent unauthorised access and data loss.

Desired Outcome 7.3 – Securing Connections: A financial institution should ensure that its networks and connections are protected from unauthorised access, resilient against exploitation or disruption, and data is transmitted securely.

Desired Outcome 7.4 – Securing the Virtual Environment: A financial institution should ensure that the virtual environments it operates in are protected from unauthorised access and data loss.

Desired Outcome 7.5 – Updating the Environment: A financial institution should ensure that its firmware and software are kept up to date in a safe and timely manner.

Chapter 8 – Data Lifecycle Management

Desired Outcome 8.1 – Data Governance: A financial institution should have organisational structures to support sound governance of data.

Desired Outcome 8.2 – Data Lifecycle Management: A financial institution should safely and securely manage its data from inception to destruction.

Desired Outcome 8.3 – Handling Data with Regulatory Obligations: A financial institution should ensure it complies with all applicable regulatory obligations pertaining to its data.

Chapter 9 – Resilience

Desired Outcome 9.1 – Availability Architecture: A financial institution should architect its systems, networks, and data to meet its availability objectives.

Desired Outcome 9.2 – Continuity Planning: A financial institution should have business continuity plans in place to minimise the impact of disruptions on its ability to deliver financial services.

Desired Outcome 9.3 – Recovery Planning and Testing: A financial institution should recover from disruptions promptly and safely.

Chapter 10 – Cyber Event Management

Desired Outcome 10.1 – Threat Awareness: A financial institution should stay apprised of the latest cyber threats to its IT environment.

Desired Outcome 10.2 – Cyber Event Lifecycle Management: A financial institution should ensure cyber events are managed to resolution promptly and safely.

Desired Outcome 10.3 – Security Testing: A financial institution should validate its ability to prevent, detect and be resilient against cyber threats.

Section C: Interacting Securely

Chapter 11 – Access Management

Desired Outcome 11.1 – Credential Management: A financial institution should ensure that credentials used to access its assets and networks are valid.

Desired Outcome 11.2 – Authorisation: A financial institution should ensure that access to its assets is managed and authorised on a least-privileged basis.

Desired Outcome 11.3 – Authentication: A financial institution should only allow access to its assets, appropriate to the authorised scope of activities, upon successful authentication of credentials.

Chapter 12 – Online Transaction Security

Desired Outcome 12.1 – Online Transaction Security: A financial institution should design its systems and processes with the aim of reducing the potential for fraudulent activity taking place via its online financial services.

Desired Outcome 12.2 – Fraud Mitigation: A financial institution should implement capabilities to detect and mitigate fraudulent activities on its online financial services.

Desired Outcome 12.3 – Customer IT Risk Awareness: A financial institution should regularly inform customers of the risks associated with the use of online financial services.

Chapter 13 – Cryptography

Desired Outcome 13.1 – Cryptographic Schemes: A financial institution should implement secure cryptographic schemes.

Desired Outcome 13.2 – Key Lifecycle Management: A financial institution should ensure cryptographic keys are managed securely throughout its lifecycle.

Section D: Leveraging Business Embedded Technologies

Chapter 14 – Algorithm Driven Solutions

Desired Outcome 14.1 – Governance of Algorithm Driven Solutions: A financial institution should have appropriate governance structures to support sound development and usage of algorithm driven solutions.

Desired Outcome 14.2 – Safe Development and Usage: The use of algorithm driven solutions should not compromise a financial institution's ability to conduct its business operations or services to customers in accordance with applicable laws and its ethical norms.

Chapter 15 – Decentralised Infrastructure Solutions

Desired Outcome 15.1 – Understanding Decentralised Infrastructure Solutions: A financial institution should establish a clear understanding of the nature and nuances of each decentralised infrastructure solution it interacts with.

Desired Outcome 15.2 – Secure Participation: A financial institution should ensure that its resources interacting with the decentralised infrastructure solution are securely managed.

Applicability

ix. While the Guidance is relevant to all financial institutions conducting regulated activities in the ADGM, it should not be interpreted as a binding set of rules for financial institutions, or a standard of care owed by financial institutions to their customers.

x. Financial institutions are expected to adapt the Guidance in a manner that is commensurate with their level of risk and complexity, taking into account the diverse activities they engage in and the markets in which they provide services to customers.

xi. Several chapters in this Guidance refer to the formation of decision-making forums or committees. The FSRA understands that this may be onerous for smaller financial institutions that have limited resources. Financial institutions are expected to assess and adopt the most suitable mechanism to achieve the objective of ensuring that processes are in place to prevent individuals from acting without the appropriate approvals.

xii. At various points in this Guidance, where reference is made to conducting due diligence on vendors, service providers, or any IT third party, financial institutions should refer to the Chapter on IT Third Party Management.

xiii. Capitalised terms contained in this Guidance have the meanings attributed to them in the FSRA's Glossary ("GLO"), unless otherwise defined in this paper.

Building Effective Control Environments

xiv. When building an effective IT risk management environment, financial institutions should have an understanding of the approach for ensuring its controls to mitigate risks are effective. Broadly, the following are applicable across the best practices described in this Guidance.

a. A financial institution should document its approach, framework, policies, and procedures and controls to mitigate a risk, commensurate to its risk appetite and business needs.

b. Controls aligned to the above documentation should be implemented with adequate resources.

c. Processes should be in place to monitor the operational effectiveness of the controls.

d. Any changes to controls should be approved by a competent party at an appropriate level of management.

e. On a regular basis, reviews should be performed and documented by a competent party to identify control lapses, weaknesses, or enhancements and vulnerabilities. Suitable actions should then be taken to remediate these findings in a timely manner commensurate with the associated risk.

f. Validation of the effectiveness of the controls should be performed on a regular basis by competent parties sufficiently distant from the operation of the control (e.g., internal audit, external audit, etc.).

xv. When adopting technologies to supplement business operations or services to customers, financial institutions may find that it is more effective to automate or embed

risk controls that have traditionally been carried out manually. Financial institutions should ensure that the documentation of their control environment takes such embedded or automated controls into account.

SECTION A: ESTABLISHING A CULTURE OF EFFECTIVE IT RISK MANAGEMENT

Chapter 1 – Governance and Oversight

Desired Outcomes for Governance and Oversight

Desired Outcome 1.1 – Strategy Alignment: A financial institution should ensure that its IT strategies are aligned with and support its overall business strategy.

Desired Outcome 1.2 – Competence: The Governing Body and senior management of a financial institution should ensure that its staff, and any third parties, are competent to perform their roles.

Desired Outcome 1.3 – Accountability: A financial institution should ensure that the appropriate staff are accountable for the management of IT risks.

Desired Outcome 1.1 – Strategy Alignment

1.1.1 Aligning IT strategies with the business strategy is a key means for financial institutions to reduce IT risk. Systems and datasets that are not fit for purpose may expose the financial institution to greater risk than desired.

1.1.2 The Governing Body of a financial institution is responsible for ensuring that the financial institution's IT strategies are aligned with the financial institution's business strategy. This is in line with the Governing Body's responsibility for setting and/or approving the business objectives of the financial institution.

1.1.3 The senior management of a financial institution is accountable to the Governing Body for ensuring that the implementation of the IT strategies effectively supports the business strategy. In turn, the Governing Body of the financial institution is responsible for providing the senior management with sufficient authority and resources to effectively implement the strategy.

Desired Outcome 1.2 – Competence

1.2.1 The Governing Body and senior management should both have members who can understand and manage IT risks that the financial institution is exposed to. This is in line with the Governing Body's obligation to provide effective oversight of the management of the financial institution. Depending on the nature, scale and complexity of IT in use, a financial institution should consider establishing dedicated roles, including senior management roles, for the management of IT and its associated risks (e.g., chief technology officer, chief information security officer, etc.).

1.2.2 Financial institutions should ensure that staff have the requisite skills and knowledge to perform their roles and manage IT risks effectively. This is especially so for roles where technical knowledge is necessary for staff to perform their duties.

1.2.3 The Governing Body and senior management should establish a competency framework for staff in all functions that can guide hiring, appraisal, and training decisions. The financial institution should support training and development of its staff where appropriate.

1.2.4 Similarly, competence in delivery of the product or service offered should be a factor in the selection of third parties (e.g., contractors, freelancers, hardware and software vendors, etc.) that interact with the financial institution.

Desired Outcome 1.3 – Accountability

1.3.1 Accountability incentivises staff to take action to mitigate IT risks. Lack of accountability may lead to staff being slow to act when a risk event occurs because they believe that other persons will be doing so.

1.3.2 The Governing Body is responsible for holding the senior management of the financial institution accountable for the effective management of IT risks. To this end, the Governing Body should ensure that the senior management of the financial institution:

1.3.2.a includes appointment holders that have the requisite experience and expertise to understand and manage IT risks;

1.3.2.b has developed an IT strategy that covers both the use of IT and the management of IT risks;

1.3.2.c has sufficient authority, resources, and access to the Governing Body to execute on the IT strategy; and

1.3.2.d has developed, documented, and implemented an effective framework to manage IT risks.

1.3.3 Financial institutions should clearly assign responsibility and accountability for managing IT risk to appropriate staff. This could be done through several means, including through a RACI matrix[3].

1.3.4 Financial institutions should identify a clear owner of each source of technology or data risk ('risk source') who is accountable for risk events ('risk owners'). Risk sources include systems, datasets and third-party arrangements. This will ensure a clear line of accountability when a risk event occurs.

1.3.5 Financial institutions should clearly set out the impact of a risk event to affected consumers, the financial institution and to staff. Clearly understanding what consequences a risk event may have, especially for individual staff, will incentivise staff to treat IT risk seriously. Financial institutions should ensure that the impact described

[3] A RACI Matrix is a commonly used approach for defining which staff are Responsible or Accountable for a task, as well as which staff should be Consulted on or Informed of the progress of the task.

is realistic and proportionate to the risk event[4], so that staff are not incentivised to hide risk events for fear of excessive penalties.

[4] For example, an email sent to the wrong address should not carry the same impact as a failure of mission-critical systems.

Chapter 2 – Risk Management

Desired Outcomes for Risk Management

Desired Outcome 2.1 – Risk Awareness: The Governing Body and senior management of a financial institution should foster a culture of IT risk awareness throughout the organisation.

Desired Outcome 2.2 – Risk Awareness Training: A financial institution should train its staff appropriately to mitigate IT risks.

Desired Outcome 2.3 –Risk Assessment Framework: A financial institution should put in place a risk assessment framework that identifies and assesses IT risks, and implements controls commensurate with the severity of the risks.

Desired Outcome 2.4 – Risk Monitoring: A financial institution should put in place a process to regularly monitor risk sources to ensure that the risk controls are functioning as designed.

Desired Outcome 2.5 – Incident Management: A financial institution should put in place procedures to detect, respond to and recover from incidents.

Desired Outcome 2.6 – Problem Management: A financial institution should establish a practice of studying past incidents and performance issues in a holistic manner to reduce the likelihood of future occurrences.

Desired Outcome 2.7 – Insider Risk: A financial institution should take steps to mitigate against insider threats.

Desired Outcome 2.1 – Risk Awareness

2.1.1 Risk awareness is the most important defence that financial institutions have against IT risks. Staff that are aware of risks can act to prevent risk events from occurring. Conversely, staff that are not aware of risk may engage in risky behaviour because they do not understand the consequences of that behaviour. For example, staff may inadvertently send emails containing unencrypted personal data to unintended recipients because they are not aware of the importance of protecting personal data.

2.1.2 A risk event is an occurrence that could pose a risk to the confidentiality, integrity or availability of a financial institution's systems and datasets. This differs from incidents, which are risk events that actually impact the financial institution's systems and datasets. For example, a power failure in a financial institution's data centre is a risk event. The power failure turns into an incident if it is not appropriately addressed by risk controls (such as backup power generators) and a disruption to the financial institution's systems and data occurs.

2.1.3 Fostering a culture of risk awareness is crucial for the financial institution. In such a culture, staff are aware of the risks that they face and use IT securely to achieve business objectives. Financial institutions should avoid the extreme of risk aversion,

where staff avoid taking any risk regardless of the impact on the business, or risk blindness, where staff disregard potential risks in pursuit of business objectives.

2.1.4 The Governing Body and senior management of a financial institution should foster a culture of risk awareness throughout the financial institution by setting the 'tone from the top'. This can be done by demonstrating a personal commitment to mitigating IT risk. Staff are unlikely to take IT risk seriously if they see that the Governing Body and senior management do not act in line with the financial institution's stated practices for IT risk.

2.1.5 For example, a culture of open reporting of incidents can significantly aid financial institutions in building a culture of risk awareness. By reporting all incidents, no matter how minor and including 'near misses', financial institutions can identify and mitigate patterns of problems in risk management practices so that they can respond to potential incidents in a timely manner and identify issues before further risk events occur. For a culture of open reporting to work in practice, the Governing Body and senior management should create an environment where all staff are comfortable with and motivated to flag out gaps in IT risk management. The Governing Body and senior management should regularly reiterate the need to learn from such incidents and rectify problems, rather than assigning blame.

2.1.6 Financial institutions should put a framework in place to monitor staff awareness of IT risk. This framework should include both qualitative factors, such as staff perception of IT security, as well as quantitative factors, such as the number of risk events experienced by the firm. The monitoring framework should be reviewed on a periodic basis to ensure that its contents and factors remain relevant.

2.1.7 The results of the monitoring framework should be reviewed regularly to identify both lessons learnt as well as steps that can be taken to improve awareness.

Desired Outcome 2.2 – Risk Awareness Training

2.2.1 To effectively mitigate IT risks, staff should be appropriately trained. Without such training, staff may either make the occurrence of a risk event more likely or worsen the impact of a risk event.

Regular and Relevant Training

2.2.2 Financial institutions should put in place a comprehensive training program that raises awareness of IT risks and gives staff appropriate training to mitigate risks that they may commonly face in their day-to-day activities. The training program should be proportionate to the nature, scale and complexity of the financial institution and should minimally cover:

2.2.2.a the financial institution's policies and standards;

2.2.2.b the specific IT risks, including in particular the cybersecurity risks, that staff are exposed to;

2.2.2.c staff's responsibility and accountability for mitigating IT risk and reporting risk events;

2.2.2.d steps that staff can take in their day-to-day work to mitigate IT risk; and

2.2.2.e any applicable laws, regulations or guidance relating to IT risk.

2.2.3 Financial institutions should tailor the contents of the training program to meet the needs of specific groups. For example, the needs of the Governing Body and senior management or of IT staff will differ from those of general staff. In particular, high-risk groups, such as those with privileged system access or in sensitive business functions, should be identified and receive targeted security awareness training.

2.2.4 Financial institutions should conduct the training program for all staff, be they permanent or temporary, on a regular basis. For new staff, financial institutions should conduct the training program as soon as is practical after they join the organisation.

2.2.5 Financial institutions should review the training program on a periodic basis to ensure that it remains relevant and effective by taking into account emerging risks and changes in the IT risk landscape.

Desired Outcome 2.3 –Risk Assessment Framework

2.3.1 It is not possible to prevent all risk events from occurring. However, implementing a structured and comprehensive risk management framework can help a financial institution prevent common risk events and reduce the likelihood and impact of unforeseen risk events.

2.3.2 In addition to the key risks highlighted in the Introduction, financial institutions are exposed to several domains of potentially overlapping enterprise-level IT risks, including:

2.3.2.a **Project management risk** – the risk that a technology or data project will fail to meet desired outcomes;

2.3.2.b **IT operations risk** – the risk of an unexpected compromise to a system or dataset's confidentiality, integrity or availability. This includes unexpected system behaviour or errors e.g., due to incorrectly applied patches;

2.3.2.c **Data security risk** – the risk of a dataset experiencing a disruption to its confidentiality, integrity or availability, whether by attack or by unexpected behaviour. Data security risk differs from cybersecurity and IT operations risk because it takes into account the content of the data;

2.3.2.d **Cybersecurity risk** – the risk of an attack on a system that disrupts its confidentiality, integrity or availability. Cybersecurity risk differs from operations risk because of the need to consider the threat model and attacker; and

2.3.2.e **Third-party risk (IT-focused)** – the risk of compromise to a system or dataset's confidentiality, integrity or availability as a result of weak controls in a third party that the financial institution has dealings with.

2.3.3 A risk event in one domain can affect other domains. For example, a cybersecurity risk event caused by an external attacker could compromise the confidentiality of a dataset and the availability of the system containing that dataset. Financial institutions should therefore consider all relevant domains when assessing the risk to each system or dataset.

2.3.4 While IT risks pose their own unique challenges, they contribute to the larger category of operational risks[5]. Treating IT risks as a separate exercise could lead to gaps in risk controls. As such, financial institutions should account for and integrate the management of IT risks as part of their overall management of operational risk. Staff tasked with managing IT risk should be regularly apprised of and included in the governance structures for managing operational risk.

Governance Structures

2.3.5 Financial institutions should put in place governance structures appropriate for their nature, scale and complexity to:

2.3.5.a oversee the development of the risk assessment framework;

2.3.5.b regularly review the risk assessment framework to ensure its adequacy and effectiveness;

2.3.5.c establish, maintain and implement sound policies and processes for managing IT risk;

2.3.5.d identify and assign accountability for risks; and

2.3.5.e manage IT risks in accordance with the risk assessment framework and the IT strategies.

2.3.6 Financial institutions should conduct regular and independent assessments of the effectiveness of the governance structures, their management of risk and their risk controls. Such assessments may be conducted by the financial institution's internal audit functions or by external auditors.

2.3.7 Financial institutions should define a lifecycle for their risk assessment framework that includes at least the stages set out in GEN Rule 3.3.4; identify, assess, mitigate, control and monitor.

[5] As defined in FSRA Rulebooks, consistent with definitions provided by the Basel Committee on Banking Supervision, operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.

2.3.8 Financial institutions should ensure that the risk assessment framework has a common definition and measure of risk across all domains. For example, a financial institution may define risk as the product of likelihood and impact and use the same measurement scale to measure likelihood and impact across all domains. This will provide a common basis for financial institutions to assess risk and reduces the likelihood that IT and business teams have a different understanding of the severity of any risk rating.

Risk Acceptance

2.3.9 It is rarely possible to both eliminate all risk and meet business objectives. Even after controls have been put in place to mitigate a risk, a residual risk may remain. In some cases, it may not be feasible to put risk controls in place in the short term, such as for legacy systems that are out of support. In such cases, the residual risk will remain until a more long-lasting risk control is implemented, such as replacing the legacy system.

2.3.10 To manage residual risk effectively, the Governing Body and senior management should have a well-articulated risk appetite/tolerance that can guide decision making throughout the financial institution. Consequently, all key IT decisions should align with the financial institution's risk appetite/tolerance, with exceptions allowed only in extraordinary circumstances, such as emergencies, and subject to approval at an appropriate level of management.

2.3.11 Financial institutions should ensure that risk owners are aware of the inherent risk and the current residual risk for their risk sources. Financial institutions should implement controls to reduce the residual risk to an acceptable level consistent with the established risk appetite/tolerance or replace the risk source with an acceptable alternative.

2.3.12 For residual risk acceptance, financial institutions should have a process in place for the risk owner to seek approval from an appropriate level of management or from the Governing Body depending on the risk to be accepted.

2.3.13 Financial institutions should ensure that risk owners' accountability is commensurate with their authority and competence. For example, senior management should avoid assigning accountability for material or critical risk sources to staff who are not trained or do not have the requisite experience to manage such risks.

2.3.14 As part of its risk management framework, the financial institution may consider obtaining insurance coverage for IT risk events. While such a risk management measure can aid the financial institution in weathering the financial impact of risk events, it should not be used as a crutch to absolve the financial institution of its responsibility to implement robust controls to prevent risk events from occurring.

Risk Register

2.3.15 Financial institutions should have an accurate and up-to-date register of IT risks it is exposed to. The register should record:

2.3.15.a the risk owner for the risk;

2.3.15.b a description of the risk;

2.3.15.c the materiality of the risk to the financial institution;

2.3.15.d risk indicators with thresholds that would trigger actions to be taken by the financial institution;

2.3.15.e controls applied to mitigate the risk and the residual risk; and

2.3.15.f whether the risk owner has accepted the residual risk, if any.

2.3.16 Financial institutions should regularly update the register in response to changes to the risk sources as well as changes in the IT or business environment. This will ensure that there is a common understanding of the risks faced by the financial institution. The financial institution should also make a record of what changes have been made to the register to track the evolution of the financial institution's risk profile.

Desired Outcome 2.4 – Risk Monitoring

2.4.1 Risk controls may not always function as intended and changes in the environment could degrade their effectiveness. This could lead to financial institutions having a false sense of security, being exposed to more risk than is acceptable. It is therefore crucial that financial institutions monitor the effectiveness and adequacy of their risk controls on an ongoing basis.

2.4.2 Financial institutions should define metrics to measure the effectiveness of their risk controls. As far as possible, financial institutions should seek to use common metrics across multiple risk sources, as well as augmenting these common metrics with risk source-specific metrics where needed. The metrics should include both quantitative measures as well qualitative measures of effectiveness. Such metrics should at a minimum take into account risk events that have occurred or been averted, observations raised by auditors or regulators as well as applicable regulatory requirements.

2.4.3 Financial institutions should put systems and processes in place to collect the control effectiveness metrics in an accurate and timely manner. The systems and processes should be regularly reviewed and updated to ensure that they continue to collect metrics in an accurate and timely manner.

2.4.4 Financial institutions should regularly review the control effectiveness metrics that they have collected to determine whether their risk controls have been effective at preventing or reducing risk. Based on this review, financial institutions should update their risk controls to address deficiencies in effectiveness. Financial institutions should take the severity of the deficiencies as well as the impact of the changes on other risk controls and risk sources into account when planning these updates.

2.4.5 Where a control repeatedly fails to achieve its expected effectiveness metric, a financial institution should review the design of the control to determine the root cause of the failure and take appropriate steps to implement alternative controls or processes that address the attendant risks.

Desired Outcome 2.5 – Incident Management

2.5.1 Even though risk controls can be put in place to minimise occurrence, it is not possible to prevent all risk events from materialising. It is therefore crucial that financial institutions establish controls and processes that allow them to detect, respond to and recover from materialised risk events i.e., incidents, in a timely way.

2.5.2 During the early stages of an incident, it is often hard to obtain clear and actionable information. Erroneous information can often propagate. Having a well-structured process for responding to an incident lets financial institutions focus on decision making. Clear communication is equally essential, to prevent the spread of misinformation that could cause erroneous decisions to be taken.

2.5.3 Financial institutions should have an incident management framework in place to ensure that incidents are dealt with swiftly and effectively, including:

2.5.3.a how the financial institution should investigate risk events, in particular in maintaining and protecting evidence should a risk event be an incident;

2.5.3.b how the financial institution classifies the severity of each incident;

2.5.3.c what processes the financial institutions has for detecting, responding to and recovering from different types of incidents such as cyber-attacks or software failure;

2.5.3.d who is responsible for what role in detecting, responding to and recovering from incidents;

2.5.3.e which stakeholders should be updated, at what point the stakeholders should be updated during the incident and what information should be shared with the stakeholders; and

2.5.3.f defined criteria for when the incident's severity warrants activation of business continuity plans and convening of crisis management teams for prompt decision making.

2.5.4 Financial institutions should regularly review, test, and update the framework to ensure that it remains relevant and effective.

Incident Detection

2.5.5 Financial institutions should put systems in place to detect risk events when they occur. Financial institutions should also put processes in place to allow reporting of risk events

by staff and by external parties. These systems and processes should capture the risk event's nature and scale.

2.5.6 Incidents may occur at any time and at any system in the financial institution's technology implementation. A financial institution should monitor all hardware, software, networks, and connections for risk events.

2.5.7 Financial institutions should regularly broadcast the incident management framework to ensure that staff are apprised of incident reporting procedures and informed of lessons learned from manifested risk events in a timely manner.

Incident Investigation and Escalation

2.5.8 Financial institutions should promptly investigate risk events to ascertain their nature and scale, and to verify whether a risk event is an incident.

2.5.9 If the risk event has been confirmed to be an incident, financial institutions should promptly assess the incident to assign it an initial severity. Financial institutions should continue to assess the incident as it develops to determine if a higher or lower severity is warranted.

2.5.10 A financial institution should ascertain the scope of the incident's impact and quickly contain the impact of the incident e.g., by isolating affected resources from the rest of the IT environment, redirecting network traffic to unaffected resources, ensuring backups are only restored from versions not impacted by the incident, etc.

2.5.11 Financial institutions should ensure that there are adequate resources available at all times to respond to incidents. As incidents can occur at any time, financial institutions should make necessary arrangements internally or through third parties to perform the necessary investigations during incidents. The incident management framework should account for any third parties involved and require performance and reporting outcomes.

Response and Recovery

2.5.12 If the incident is expected to have or has already made a material impact on business operations and/or services to customers, a financial institution should ensure that the Governing Body and senior management are regularly apprised of the situation and provided with adequate information to make a decision on whether or not to activate business continuity plans.

2.5.13 As part of its incident management framework, a financial institution should establish an incident playbook comprising approved and validated steps to be taken to respond to common incidents. Such a playbook reduces the time to action when an incident occurs and provides a consistent reference point. The incident response playbook should be regularly tested and updated to ensure it remains effective, and aligned with the financial institution's business continuity and disaster recovery plans.

2.5.14 Once a financial institution has recovered from an incident, whether material or not, it should conduct an after-action review to identify the root cause(s) of the incident and interventions that could have prevented or mitigated the impact of the incident. Financial institutions should translate applicable lessons learnt from the after-action review process into improved procedures for personnel to follow, enhanced controls to be implemented, and/or changes to systems to close vulnerabilities.

Communication Plan

2.5.15 As part of its incident management framework, financial institutions should have a clear communication plan in place to update relevant stakeholders during an incident. Financial institutions should at a minimum include the Governing Body, senior management, media, customers and the general public as relevant stakeholders.

2.5.16 The communication plan should set out what messages the financial institution intends to convey, at what point these messages will be sent and to whom the messages will be sent both internally and externally. It should also set out what coordination points the financial institution intends to set up with its stakeholders. Where possible, the communication plan should include pre-defined statements for release to media or for public queries.

2.5.17 Financial institutions should regularly update their communication plans to ensure that the messages and recipients remain accurate and relevant. This will make the spread of misinformation and confusion less likely.

2.5.18 Financial institutions should ensure that the relevant staff are aware of the communication plan and their responsibilities in executing the plan. This will make conflicting messages less likely, reducing confusion.

2.5.19 During an incident, the financial institution should deviate from the communication plan only where the consequences of deviation are understood and accepted by senior management.

Incident Reporting

2.5.20 A financial institution should establish procedures and escalation frameworks to facilitate compliance with incident reporting obligations in the prescribed format required by regulators and other authorities.

2.5.21 Where the incident is potentially the result of or part of a crime, the financial institution should make a report to law enforcement authorities[6] and fully facilitate the investigation process, including maintaining the chain of evidence for any systems or data involved in the incident.

Contractual Obligations

[6] This may include filing the necessary submissions (e.g., suspicious transaction reports, etc.) to report potential financial crimes to the appropriate authorities (e.g., financial intelligence unit, etc.).

2.5.22 A financial institution should have procedures in place to ascertain the potential for an incident to result in breaches to its contractual obligations to customers and counterparties.

2.5.23 Where a breach occurs, a financial institution should notify the affected party and take necessary steps to mitigate further escalation of its non-performance.

Desired Outcome 2.6 – Problem Management

2.6.1 Investigations into the root cause of risk events can glean lessons for improvement but such lessons will be wasted if they are not acted on. Financial institutions should have a process in place to study lessons learnt over time to identify, analyse, and resolve systemic problems. The goal of problem management is to reduce the likelihood of a risk event materialising into an incident or to minimise the frequency and severity of potential and actual risk events.

2.6.2 The financial institution should regularly review risk events to identify potential problems, determine mitigation strategies and report the results of its review to management for approval and action. A repeated risk event that does not turn into an incident may become normalised and may slow response when an incident does occur. For example, repeated false alerts from intrusion detection solutions may lead staff to ignore such alerts, even when an attacker has already entered the network.

2.6.3 In addition to technical factors that led to risk events, the financial institution should also identify any underlying issues that may originate from lack of compliance by staff to existing frameworks and processes, inappropriate or deficient processes, and unresolved or ignored user service requests.

Desired Outcome 2.7 – Insider Risk

2.7.1 Malicious insiders can be a significant source of IT risk as their insider knowledge enables them to easily circumvent internal controls[7].

2.7.2 While the risk of malicious insiders can never be eliminated, financial institutions should conduct background checks on staff and third parties who have access, especially privileged access, to data and systems. The intensity of the background check should be commensurate to the level of access granted to the staff.

2.7.3 Financial institutions should also implement systems and processes to monitor for insider risk (e.g., data exfiltration, resource abuse, etc.).

[7] Per the causal factors that comprise the Fraud Triangle, removal of weak internal controls to reduce the Opportunity for fraud is a key deterrence to combat fraud.

Desired Outcomes for Third Party Management

Desired Outcome 3.1 – Third Party Risk Governance: A financial institution should ensure that its engagement with third parties aligns with its business strategy and adheres to the established risk management framework.

Desired Outcome 3.2 – Third Party Lifecycle Management: A financial institution should closely monitor and review its third parties' performance and risk posture.

Desired Outcome 3.3 – Supply Chain Resilience: A financial institution should actively monitor and mitigate risks arising from its third parties' supply chain.

Desired Outcome 3.1 – Third Party Risk Governance

3.1.1 For the purposes of this chapter, a third party is any entity that provides or consumes technology services or products to or from the financial institution.

3.1.2 A financial institution may engage third parties for various purposes including for reasons such as cost efficiency or to leverage on an established expertise. As risk events impacting third parties can in turn impact financial institutions, these relationships need to be managed and associated risks mitigated effectively.

3.1.3 Regardless of how the financial institution assigns liability to its third parties through contractual arrangements, the financial institution is ultimately accountable to its customers and stakeholders for any risk events that impact them. A financial institution cannot absolve itself of its responsibility for managing risks arising from third party arrangements.

Oversight and Accountability

3.1.4 As the Governing Body is ultimately responsible for the financial institution's activities, a financial institution should include third party risk management as part of its risk management framework, with adequate reporting by senior management to the Governing Body.

3.1.5 A financial institution should establish a third-party management framework that governs management of third parties throughout their lifecycle. A forum with appropriate management representatives should be established for decision making pertaining to third party arrangements and changes to the third-party management framework. Each third-party arrangement should be overseen by a competent individual or function within the financial institution to facilitate monitoring of the third party's performance.

3.1.6 For financial institutions that rely on intra-group or related entities for products or services, the financial institution should establish processes that enable it to have effective oversight and the ability to influence the products or services provided to it by

the intra-group entities. The financial institution should establish formal agreements with the intra-group or related entities to clearly demarcate between dedicated and shared resources. The financial institution should be able to manage third party risks specific to itself as it is still responsible for its operations and services to its customers. The financial institution should also ensure that the intra-group or related entities comply with its regulatory obligations.

3.1.7 A financial institution's third-party management framework should include key performance indicators with thresholds that senior management use to track and monitor the performance and risk posture of all its third-party arrangements. Such indicators should be meaningful for decision making and should not be limited to financial metrics.

3.1.8 A financial institution should maintain a register of all third-party arrangements that is readily accessible for review by the Governing Body and senior management. The register should be updated on a timely basis and reviewed regularly to ensure information on the third parties are up to date.

3.1.9 A financial institution should also consider concentration risk when determining the suitability of a third party. While there are benefits to engaging third parties that service a large number of financial institutions and unavoidable in some scenarios (e.g., utilities, telecommunications, financial transaction messaging, etc.), financial institutions should be cognisant of the potential risks arising from being party to third party arrangements that exhibit high concentration risk. The following are some ways in which third party concentration risk can manifest and have a significant impact should a risk event result in a disruption to the concentrated product or service.

3.1.9.a A financial institution relying on a single third party for multiple products or services (e.g., online workspace application service providers).

3.1.9.b A financial institution that has multiple third parties relying on a single fourth party (e.g., web hosting service providers).

3.1.9.c Multiple financial institutions relying on a single or few third parties for products or services (e.g., computer hardware, web services, etc.).

Materiality

3.1.10 A financial institution's third-party management framework should include procedures for assessing the materiality[8] of a third-party arrangement.

[8] The definition of materiality follows the Guidance following GEN Rule 3.3.32 for outsourcing arrangements. As additional guidance and for arrangements not considered outsourcing, a third-party arrangement is material when a financial institution assesses that a potential risk event occurring at the third-party results in a significant financial loss to the financial institution, a significant disruption to a financial institution's ability to conduct business or service customers, a significant impact on a financial institution's reputation, or a significant impact to the financial institution's ability to comply with legal and regulatory obligations.

3.1.11 A financial institution should ensure that the materiality assessments of its third-party arrangements are reviewed regularly by its senior management to account for any changes in the nature, scope, or complexity of the arrangements.

3.1.12 A financial institution should perform more stringent due diligence and have greater requirements for the ongoing monitoring of its material third party arrangements.

Outsourcing

3.1.13 For the purposes of this Guidance, an outsourcing arrangement in the context of the financial institution is an arrangement where a third party is engaged to perform tasks, functions, processes, services or activities that would otherwise be undertaken by the financial institution itself. For example, a technology vendor developing and hosting the platform that the financial institution's customers would perform financial transactions on, or a third party that conducts electronic know-your-customer checks during client onboarding.

3.1.14 A financial institution should be cognisant of the impact to itself in the event a third party is unable to demonstrate a satisfactory level of performance, encounters an adverse development, or practices poor risk management practices resulting in material risk events. A financial institution should be able to make alternative arrangements to mitigate this risk including potentially re-integrating the outsourced service.

Desired Outcome 3.2 – IT Third Party Lifecycle Management

3.2.1 A financial institution's third-party management framework should include procedures that enable the financial institution to have strong oversight throughout the lifecycle of each third-party arrangement.

Due Diligence

3.2.2 A financial institution's third-party management framework should have procedures for the assessment of each third-party arrangement prior to entering into such arrangements. The assessment should consider if each third-party arrangement is in line with the overall business and IT strategy, and that engagement with each third party would not detrimentally impact the risk profile of the financial institution. The assessment should also include comprehensive due diligence on each third party and its ability to perform, as well as any regulatory or legal obligations the third party should be compliant with.

3.2.3 A financial institution should ensure that adequate due diligence is performed on third parties and approved at an appropriate level of management. While the extent of the due diligence may vary depending on the nature of each third-party arrangement, a financial institution should consider the following and document the due diligence performed.

3.2.3.a Track record of the third party in performing the activity and its ability to continue doing so for the contract period;

3.2.3.b Financial viability of the third party;

3.2.3.c Business profile in the industry and any adverse developments such as legal action or negative media coverage;

3.2.3.d Quality of products or services involved in the arrangement, how the products or services meet the financial institution's requirements, and comparison with peer products and services in the market;

3.2.3.e Availability and location(s) of human resources within the third party to support the delivery of products or services to the financial institution;

3.2.3.f Types of data to be transferred between the financial institution and the third party and the security controls in place to mitigate associated IT risks;

3.2.3.g Management of IT risks by the third party for the activities relevant to the arrangement;

3.2.3.h Threat and vulnerability management processes to mitigate known exploits in a timely manner;

3.2.3.i Resilience measures, recovery objectives where applicable, and incident escalation protocols between the third party and the financial institution;

3.2.3.j Impact on the financial institution and its customers should the third party fail to perform or encounter a risk event;

3.2.3.k Independent validation and/or certification of control implementation within the third party;

3.2.3.l Resilience of the third party's supply chain, including sub-contracting, which supports the activities relevant to the arrangement;

3.2.3.m Ability for the financial institution to conduct audits on the third party and its sub-contractors, or to obtain audit reports from the third party and its sub-contractors;

3.2.3.n Ability to comply with regulatory obligations; and

3.2.3.o Other relevant factors e.g., political, economic, social, and legal considerations of the jurisdictions that the third party operates in.

3.2.4 Where a third party is providing human resources (e.g., freelance software developer, contract IT support staff, etc.), the financial institution should ensure that these individuals would not pose a higher risk to the financial institution than its own employees. For example, a financial institution that does not hire persons who have a record of criminal convictions or bankruptcies should take into consideration if third party individuals have a similar record.

3.2.5 Where the third-party arrangement is an online service that has fully automated the onboarding, usage, and exit of the arrangement, the financial institution should nonetheless perform sufficient due diligence to ascertain the suitability of subscribing to the online service.

Third Party Contractual Agreements

3.2.6 A financial institution should ensure that the contractual agreement between it and a third party addresses any concerns highlighted during the due diligence in addition to provisions governing the products or services involved in the arrangement.

3.2.7 A financial institution should ensure that all third-party arrangements are governed by formal documented contracts that describe the terms, conditions, obligations, responsibilities, dispute management, rights and expectations of the contracting parties. Such contracts should be vetted on their legality and enforceability by a competent party.

3.2.8 Where a third-party engaged by the financial institution chooses to use sub-contractors to perform the contracted service, the third-party should ensure that the sub-contractors adhere to performance expectations and comply with regulatory obligations. The third-party should notify the financial institution of any changes in sub-contracting of the contracted service.

3.2.9 In particular, for the management of data risks, where the third party has access to, processes, or stores the financial institution's customers' data, the contractual agreement should have the necessary provisions to oblige the third party to comply with data protection regulations applicable to such data, and other applicable regulations.

Monitoring

3.2.10 The responsible individual or function within a financial institution should closely monitor the financial institution's third-party arrangement(s) to ensure the third party meets expectations and the extent of monitoring should be commensurate with the nature, scope and complexity of the third-party arrangement. For example, monitoring can take the form of real-time monitoring of key metrics on service levels, regular reports provided by the third party on the performance of its product(s) or service(s), or meetings with the third party to resolve operational, risk management, or regulatory concerns.

3.2.11 As each third party is itself a live business entity that makes its own decisions on business strategy and risk management, financial institutions should not treat third parties as unchanging or static. Once entered into arrangements, a financial institution should conduct due diligence regularly to ensure that its third-party arrangements continue to remain relevant, effective and compliant. The regular due diligence performed on third parties should be reviewed and approved by an appropriate level of management.

3.2.12 A financial institution should include in its monitoring the regular conduct of independent audits and/or expert assessments of its third parties, or the acquisition of such reports from the third parties' independent auditor and/or expert assessor. The scope of such audits should include an assessment of the third party's and its sub-contractor's IT environment and security control implementation, incident management processes, and any regulatory obligations that the third party should comply with. The financial institution should include any outstanding findings in its regular due diligence performed on the third parties. If the outstanding findings are not promptly or adequately resolved by the third party and the associated risk exceeds the financial institution's risk appetite, the financial institution should consider terminating the arrangement.

3.2.13 Where issues arise in the course of the third-party arrangement, the responsible individual or function should promptly apprise senior management and seek guidance on the necessary actions to review the arrangement for modification or termination.

Termination

3.2.14 The financial institution's third-party management framework should have procedures in place to manage the risks arising from termination of a third-party arrangement and plan for various termination scenarios. For example, scenarios for the smooth transition of one third party to another providing the same or similar product or service, in-sourcing of an outsourced activity, or the abrupt termination of a third-party arrangement. Regardless of scenario, the financial institution should ensure that it is able to continue business operations and services to customer to the fullest extent possible.

3.2.15 A financial institution should ensure that any data, documents, or records provided to the terminated third party are returned, deleted, destroyed, or rendered unusable upon termination, or as soon as practicable upon expiry of regulatory obligations on data retention.

3.2.16 Where the financial institution has implemented any technical integrations with the third-party or maintains repositories for sharing data, steps should be taken to ensure that any such integrations are disconnected and/or disabled completely. All configurations (e.g., firewall rules) made to enable access by the third-party should be revoked and closed.

3.2.17 The financial institution should ensure that all credentials and access rights to its systems and data granted to the third-party are revoked.

Desired Outcome 3.3 – Supply Chain Resilience

3.3.1 Financial institutions that rely on third parties for material activities relating to the conduct of business operations and services to customers should establish an understanding of the supply chain used by these third parties. Such an awareness would enable the financial institution to anticipate potential risk events (e.g., hardware component shortages, significant delays in shipping/transportation, operational

disruptions to major internet or telecommunications providers, etc.) and take pre-emptive action to mitigate any potential impact.

3.3.2 Where appropriate and possible, a financial institution should include diversification of third parties as part of its third-party risk management strategy to improve supply chain resilience.

3.3.3 A financial institution should also have oversight over how its data is shared with or made accessible to other parties via its third parties, in particular to ensure that such activities are carried out in line with regulatory obligations.

Desired Outcomes for Compliance and Audit

Desired Outcome 4.1 – Comply: A financial institution should include IT obligations in its compliance programme.

Desired Outcome 4.2 – Audit: A financial institution should include IT controls in its audit programme.

Desired Outcome 4.1 – Comply

4.1.1 Financial institutions should ensure that they are aware of and in compliance with the relevant regulatory expectations and requirements issued by regulators in the jurisdictions they operate in.

4.1.2 As part of its compliance framework, a financial institution should ensure that its IT policies and procedures include controls that are in line and up to date with the relevant regulatory obligations, including IT-related obligations.

4.1.3 A financial institution should ensure its compliance testing programme incorporates checks to validate its compliance with IT-related regulatory obligations.

Desired Outcome 4.2 – Audit

4.2.1 A financial institution should ensure that its audit function can provide the Governing Body and senior management an independent and objective assessment of whether the controls implemented by the financial institution can effectively mitigate IT risks.

4.2.2 The audit function should have the appropriate skills, training and experience to competently conduct assessments relating to IT risks, regardless of whether it is internal, managed by intra-group entities, or outsourced.

4.2.3 The audit programme should include IT risks and encapsulate all IT resources that support business services and functions, including those supported by third parties. In addition to control effectiveness, the audit programme should assess the adequacy of internal frameworks, policies and procedures relating to the management of IT.

4.2.4 The audit plan for IT risk should be approved by the Governing Body's Audit Committee or equivalent. The audit plan should comprise the auditable areas for each year in line with the financial institution's audit cycles. The audit cycles should be commensurate to the criticality and risks posed by the financial institution's systems, interconnections, and dependencies.

4.2.5 A financial institution should establish a process to track, escalate and monitor to resolution all audit findings related to IT.

4.2.6 Financial institutions should incorporate IT into their external audit programs to provide the Governing Body and senior management an additional independent perspective on the financial institution's management of IT risks.

SECTION B: MANAGING AN IT ENVIRONMENT

Chapter 5 – System Lifecycle Management

Desired Outcomes for System Lifecycle Management

Desired Outcome 5.1 – Project Management Oversight: A financial institution should ensure that IT projects align with its business strategy and adheres to the established risk management framework.

Desired Outcome 5.2 – System Acquisition, Development, and Testing: A financial institution should put in place a robust framework for managing the acquisition, development, and testing of systems.

Desired Outcome 5.3 – System Refresh and Decommissioning: A financial institution should establish processes to manage the safe and secure refresh and decommissioning of its systems.

Desired Outcome 5.1 – Project Management Oversight

5.1.1 A financial institution should establish a project management framework to ensure that IT projects are managed and delivered in a consistent manner that meets project and business objectives and is aligned with the financial institution's operational risk management framework. The framework should cover the rules, standards, procedures, processes and activities to manage projects from initiation to closure. The framework should also include procedures to identify, assess, treat, and monitor any project risks that may arise during the project.

5.1.2 A financial institution should ensure that staff with the appropriate authority and competence, commensurate with the scale and complexity of the project, are assigned to oversee, manage resources, coordinate between stakeholders, and approve key decisions throughout the project. The financial institution should involve relevant representatives from technical and business functions at appropriate stages of the project to provide direction and feedback to ensure project outcomes are realised in an effective and timely manner.

5.1.3 Prior to commencing the IT project, the financial institution should conduct necessary analysis to determine if there is a business need for the project, adequate funding and resources, and measurable positive outcomes on the potential impact of the system(s) on operations or services. The appropriate level of management should approve the project prior to commencement.

5.1.4 A financial institution should develop an IT project plan that sets out the scope and objectives of the project, as well as the activities, milestones and the deliverables to be realised at each phase of the project. The plan should clearly define the roles and responsibilities of staff and any third parties involved in the project.

Desired Outcome 5.2 – System Acquisition, Development and Testing

5.2.1 Depending on business strategy, financial institutions may either source for systems or develop their own systems. Each approach should be managed according to the internal rules and standards of the financial institution, and attendant risks managed in accordance with the risk management framework.

End-User Computing

5.2.2 As tools for work automation become more intuitive and as more people become proficient in the use of such tools (e.g., macros, automation scripts and tools, online services, etc.), end-user computing's ('EUC') role in addressing business needs will grow.

5.2.3 A financial institution should establish a process for staff to engage the appropriate level of management to seek approval for EUC with appropriate assessments performed on the business necessity, security posture, and performance of the EUC system or service.

5.2.4 A financial institution should incorporate approved EUC into its IT asset inventory, risk management and compliance programs, configuration and patch management processes, business continuity plans, and any other relevant IT processes and programs to ensure that approved EUCs operate under the financial institution's ongoing oversight.

5.2.5 Financial institutions should ensure that all staff are aware of the risks of procuring or developing their own systems or services without the knowledge of the IT team(s) and discourage unauthorised EUC as it may result in unexpected security gaps or corporate data exposure and expose the financial institution to risk events.

Sourcing

5.2.6 A financial institution should establish rules and procedures for the procurement of systems and due diligence of vendors. Such rules and procedures, and due diligence, should include an assessment of vendors' track record, product or service standards, alignment with required system specifications, and the vendors' ability to deliver the requisite systems.

5.2.7 A financial institution should ensure that a sourced system's (whether provided as a product or as a service) IT security and data protection standards are at least on par with the financial institution's own IT security requirements. Necessary approvals from the appropriate level of management within the financial institution should be sought if a sourced system does not meet the required IT security and data protection standards.

5.2.8 For sourced IT projects that require a vendor be granted access to the financial institution's IT environment, the financial institution should ensure that any such access is stringently assessed, granted, and monitored to prevent unauthorised access to sensitive data or introduction of malicious software ('malware') from the vendor.

5.2.9 A financial institution should have in place a process to replace a sourced system with an alternative vendor in the event of a system failure or vendor dissolution. Where only a limited number of vendors are available and there are few or no substitute systems that can meet the IT project objectives, the financial institution should assess the criticality of the system to the business and establish alternative arrangements (e.g., source code escrow, manual workarounds, etc.) to meet business needs.

Cloud Computing

5.2.10 Cloud computing service providers offer a variety of services that come with varied responsibilities depending on the service model adopted, often referred to as the 'shared responsibility model'. A financial institution should have full clarity on its responsibilities prior to subscribing to or entering into any cloud computing service arrangement.

5.2.11 Like any other sourcing or third-party arrangement, a financial institution should ensure that the cloud computing service arrangement is aligned with its business strategy and adequate due diligence is performed on the cloud computing service provider prior to entering into the arrangement.

5.2.12 In addition to the service model[9], a financial institution should choose a deployment model (e.g., public, community, private, edge, multi-cloud, hybrid, etc.) most appropriate to its needs and ensure that the cloud computing service provider at least logically segregates the financial institution's cloud deployment and data from other customers.

5.2.13 Regardless of service or deployment model, a financial institution should have clarity on the location of its workload and data at all times. As a financial institution's deployment in the cloud becomes more complex and makes use of features that may only be available in specific geographic locations, a proper accounting of assets in the cloud will prevent unaccounted assets being exploited by threat actors.

5.2.14 Given the ease in which assets can be created, deployed, altered, and removed in the cloud, financial institutions should consider adopting cloud access security broker solutions to provide visibility and control over data and threats in the cloud.

5.2.15 Where a multi-cloud strategy is adopted, a financial institution should ensure that the differences of each cloud computing service used are taken into account when developing solutions for multi-cloud deployment. A financial institution that uses abstraction tools to manage its multi-cloud deployment should be cognisant that some cloud-native security features may be missed by the abstraction tools and take mitigating actions to rectify such omissions.

5.2.16 A financial institution should ensure that it has appropriate technical competencies to operate the chosen cloud computing service(s). For example, subscription to

[9] The common service models are Infrastructure-as-a-Service ("IaaS"), Platform-as-a-Service ("PaaS"), and Software-as-a-Service ("SaaS").

infrastructure-as-a-service where it is the financial institution's responsibility to architect and build solutions requires significantly greater technical competence than a subscription to a platform-as-a-service or software-as-a-service. Additionally, expertise in the use of one cloud computing service may not translate fully to another cloud computing service.

System Development

5.2.17 A financial institution should establish a framework to ensure that all system development projects adhere to clearly defined processes, procedures, and controls for each phase of the project cycle. Such a framework should be specific to the development methodology (e.g., waterfall, agile, DevSecOps, Scrum, Lean, etc.) or tools (e.g., coding tools, documentation repositories, continuous integration and testing tools, etc.) that the financial institution uses for projects.

5.2.18 All IT projects should take IT security considerations into account throughout the development cycle. Such a security-by-design approach enables the financial institution to reduce the likelihood of gaps in security downstream when the system or service is deployed. Appropriate staff should be involved in making regular security assessments at each phase of the project to ensure security requirements are met. Such security assessments should identify and record potential threats and risks applicable to the system being developed, and the appropriate security controls for mitigation.

5.2.19 When designing the system, a financial institution should work with relevant business functions to define and document various requirements, including functional, non-functional, performance, and resilience requirements. The relevant IT staff should assess how the system being developed would fit within the existing technology infrastructure to avoid potential conflicts during testing and integration. Depending on the scale and complexity, a financial institution may consider engaging third parties to assist in designing and/or reviewing the system architecture.

5.2.20 To prevent data or system conflicts, development work should be performed in an environment physically or logically separate from the live IT environment running production systems and data.

5.2.21 A financial institution should establish procedures on versioning and change control during development to ensure detailed tracking of releases and only authorised staff have access to perform such activities.

5.2.22 During development, the financial institution may require programming activities to build software components or configurations to integrate with other systems. To ensure safe and secure development, the financial institution should establish rules and standards, procedures and best practices that would guide staff or third parties who perform programming activities. This can include hardening standards from established industry bodies, code review practices, and static or dynamic application security testing.

5.2.23 A financial institution should ensure that code repositories are regularly backed up, securely administered and accessed only by authorised personnel through strong authentication mechanisms. Code scanning and secret scanning tools should be used to identify vulnerabilities/errors and secret keys/tokens respectively. A financial institution should store secrets in secure location separate from the source code repository with stringent access controls in place.

5.2.24 A financial institution leveraging on open-source code, libraries, software or hardware should perform a compatibility and security vulnerability assessment prior to incorporation and implementation into the financial institution's environment. A financial institution's change and patch management programmes should account for the use of such open-source products and appropriate action should be taken to mitigate risks arising from open-source products that are not supported with regular updates for enhancements or security.

5.2.25 Where an open-source programme[10] is established, a financial institution should establish policies and procedures on what source code is permitted for publication and ensure that doing so would not result in threat actors being able to exploit such code to circumvent the financial institution's security controls or inadvertently expose sensitive data.

5.2.26 A financial institution that relies on a third party to perform development should obtain assurance on the development practices of the third party prior to engagement (e.g., independent audits on the third party, certifications, etc.) and have procedures in place to monitor and review the activities performed by the third party.

System testing

5.2.27 A financial institution should test each system prior to deployment into its live IT environment. As with the development stages, the testing stage should also include relevant business and security functions to ensure that the system meets the defined functional, performance, security, and resilience requirements. IT security staff should also test security controls to ensure the identified threats and risks are adequately mitigated.

5.2.28 Depending on the project, the financial institution should assess the types of testing required (e.g., unit test, input/output validation, access and authentication test, performance test, integration test, regression test, penetration test, acceptance test, etc.) and which stage of the project to perform such testing. For sourced systems, the scope and nature of testing should be commensurate to the risk profile and deployment approach.

[10] Organisations that establish an internal open-source programme allow developers to contribute code to the public as a form of support for the open-source community. Such contributions can glean benefits such as feedback for enhancing the published code which can in turn benefit the organisation.

5.2.29 A financial institution should ensure that access to test results should be stringently controlled commensurate with the potential for leakage of sensitive data, system design, or security controls.

5.2.30 To prevent data or system conflicts, systems should be tested in an environment physically or logically separate from the live IT environment running production systems and data.

5.2.31 All issues noted during testing (software bugs, configuration errors, etc.) should be tracked and resolved. Where an issue cannot be resolved, the financial institution should ensure that any deviations from the established functional, performance, security, and resilience requirements are approved by an appropriate level of management prior to system deployment in the production environment.

5.2.32 Following testing, a financial institution should ensure that all deployments and updates to the IT environment adhere to established procedures. Further guidance is provided in Chapter 7.

Desired Outcome 5.3 – System Refresh and Decommissioning

Technology Refresh Management

5.3.1 Financial institutions should avoid using outdated or unsupported systems. Financial institutions should have in place a procedure to track the lifespan, warranties, and support contracts of all systems in use, and a process to notify relevant staff of impending end-of-support dates. A financial institution can assess the system's age, performance, business alignment, and overall condition to determine whether to update, replace, or decommission systems in accordance to established procedures.

5.3.2 Where there is no alternative to the outdated or unsupported system, or if refreshing such a system poses greater risk than retaining it, a financial institution should conduct a thorough evaluation on the risks and follow its established risk acceptance processes to obtain approval for the system's continued use.

5.3.3 Where new technology is deployed or updates are made to the system, a financial institution should ensure that staff interacting with the system are adequately trained on the new or updated system, and that any data migrated during the refresh is done so safely and securely.

System Decommissioning

5.3.4 Systems that approach end-of-life may be misappropriated or accidentally lost or destroyed if there are no measures to ensure that they are disposed of properly. This can lead to potential risk events that could impact a financial institution's reputation if data is exposed by threat actors or if the uninstallation of hardware and software is not handled carefully resulting in system disruptions.

5.3.5 A financial institution should establish an asset decommissioning strategy to safely and securely decommission systems and their associated hardware, software, and data. The strategy should include a risk assessment for each system to be decommissioned and make clear what assets are to be reused, recycled or destroyed and the means to conduct those activities. All decommissioning activities should be documented to ensure compliance with any applicable regulations, including for document retention, and for future reference during investigations.

5.3.6 Where third parties are engaged for decommissioning activities, a financial institution should perform a third-party risk assessment with due attention to the service provider's track record, product or service standards, alignment with required services, and data protection standards.

5.3.7 A financial institution should ensure that any existing data on the system being decommissioned is fully wiped from the system and a chain of custody is documented to validate that the responsible party, including service providers, had performed the data wipe.

5.3.8 A financial institution should include in its asset decommissioning strategy procedures for non-tangible assets (e.g., internet domains, online subscriptions, cloud instances, network connections between the corporate network and external systems, etc.) and leased assets (e.g., multi-function printers, proprietary terminals, leased servers and network devices, etc.) to ensure that any corporate data is promptly deleted, destroyed, or rendered unusable.

Desired Outcomes for Technology Asset Management

Desired Outcome 6.1 – Asset Identification and Classification: A financial institution should know what assets it has and how critical those assets are.

Desired Outcome 6.2 – Asset Accountability: A financial institution's assets should be responsibly managed in a way that is commensurate with the criticality of the assets.

Desired Outcome 6.1 – Asset Identification and Classification

6.1.1 In the course of business, a financial institution is likely to accumulate various physical and non-physical technology assets to support its operations and services. If left unchecked, the growth in assets can heighten risk as each asset could be exploited or abused by threat actors.

6.1.2 A financial institution should have a process in place to document all acquisition, modification, movement, and decommissioning of assets. It should regularly review its list of assets to ensure the information collected is kept updated. Such documentation should enable a financial institution to track its assets and the relevant parties responsible for the asset.

6.1.3 The universe of assets that a financial institution should track includes, among other types, physical hardware (e.g., endpoints, technology infrastructure components, etc.), software (e.g., licenses, patches, libraries, etc.), datasets (e.g., customer data, transaction data, logs, etc.), online assets (e.g., internet protocol addresses, web domains, cloud assets, etc.), and cryptographic assets (e.g., encryption keys, tokens, etc.). Assets that are rented, leased, provided through subscriptions, or managed by third parties on behalf of the financial institution should be included.

6.1.4 A financial institution should establish a security classification framework for its assets to ensure that appropriate security controls are applied based on the asset's criticality and sensitivity of data associated with or contained within the asset. Appropriate alternative arrangements should be in place to deal with scenarios where replacing the asset is a risk due to its availability in the market.

Criticality Assessment

6.1.5 While a financial institution may use numerous systems to achieve its business objectives, there is likely to be a small number of systems that are essential to the core functions of the financial institution. Such systems are typically considered 'critical' as any disruption to these systems would result in significant operational failure and/or financial losses. A financial institution should apply strict requirements for confidentiality, integrity, and availability on such systems, and require a comprehensive security approach to protect them from risk events.

6.1.6 A financial institution should establish a criterion for what constitutes a critical system and an appropriate methodology to classify its systems. In building the criteria and methodology, a financial institution may take the following factors into consideration.

6.1.6.a The business function supported by the system.

6.1.6.b The level of risk posed to the financial institution if the system were to fail or be compromised. This approach involves identifying the value of the data handled by the system, potential threats and vulnerabilities, and assessing the impact and likelihood of those threats.

6.1.6.c The extent to which the system is depended upon by other systems.

Desired Outcome 6.2 – Asset Accountability

6.2.1 A financial institution should ensure that every asset is accounted for and assigned to a suitable responsible party. The responsible party should ensure that security controls applicable to the asset are implemented, configuration standards are complied with, and the asset's lifecycle is managed.

6.2.2 For assets that require access credentials, financial institutions should ensure that such credentials are held and managed by suitable responsible parties, with appropriate security controls applied for authorisation and authentication. A financial institution should have a recovery procedure in place to address scenarios where credentials to an asset are lost or irretrievable.

Desired Outcomes for Operational Infrastructure Management

Desired Outcome 7.1 – Standardising the Operating Environment: A financial institution should maintain an up-to-date library of standardised configurations that all hardware and software comply with.

Desired Outcome 7.2 – Securing the Physical Environment: A financial institution should ensure that all physical assets connecting to its networks are secured to prevent unauthorised access and data loss.

Desired Outcome 7.3 – Securing Connections: A financial institution should ensure that its networks and connections are protected from unauthorised access, resilient against exploitation or disruption, and data is transmitted securely.

Desired Outcome 7.4 – Securing the Virtual Environment: A financial institution should ensure that the virtual environments it operates in are protected from unauthorised access and data loss.

Desired Outcome 7.5 – Updating the Environment: A financial institution should ensure that its firmware and software are kept up to date in a safe and timely manner.

Desired Outcome 7.1 – Standardising the Operating Environment

7.1.1 All hardware and software require configuration. This can be for setup, functional operations, security settings, connecting to other hardware and/or software, etc. A financial institution should establish procedures to manage configuration activities for all hardware and software to mitigate the risk of misconfiguration that can lead to risk events.

7.1.2 Financial institutions should assess and determine the most suitable methodology for their technology implementation. For example, a common practice is to establish '*baseline images*' of configurations, which are pre-configured, standardised, updated regularly, and tested version of an operating system or application that can be used as a baseline for deploying new systems or instances. Such images are used to ensure that new systems or instances are consistent and configured correctly, and to streamline the deployment process. Additionally, financial institutions may consider using configuration management tools to perform updates to the images in a controlled and consistent manner.

7.1.3 Financial institutions should maintain an up-to-date library of hardware and software configuration images or templates. In establishing such libraries, financial institutions can consider recommended configuration settings from its hardware and software vendors, hardening standards from established industry bodies, and security configuration best practices from reputable security vendors and certification bodies, etc.

7.1.4 Regular reviews of the configuration images or templates should be performed to ensure that attacks from known threats (e.g., malware, software and hardware vulnerabilities, common cyber criminals' tactics, techniques and procedures, etc.) are mitigated.

Desired Outcome 7.2 – Securing the Physical Environment

7.2.1 Physical assets are the points of interaction between staff and the virtual environment in which financial services operations are performed. Physical assets can take the shape of laptops or desktop computers, mobile devices such as smartphones or tablets, portable storage devices, printers and scanners, servers, network devices, automated teller machines, internet protocol surveillance cameras, environmental sensors, etc.

7.2.2 Physical assets may contain data or provide access to data that threat actors would be keen to exploit, steal, or corrupt. Hence, securing all physical assets is critical in ensuring that the financial institution's IT are not easily compromised.

7.2.3 All physical assets should be configured in accordance to established standards and monitored for continued compliance. Regular reviews should be performed on all physical assets to ensure that up to date security configurations are applied.

7.2.4 Endpoint protection solutions (e.g., anti-virus, URL sandboxing, email attachment scanning, web browsing isolation, application whitelisting, anti-keylogging/anti-spyware, endpoint detection and response solutions, etc.) should be deployed on applicable physical assets to strengthen protection against threat actors. Where such solutions require regular updating (e.g., new virus signatures, malware behaviours, etc.), a financial institution should establish a process to perform such updates in a timely manner and validate that such updates would not disrupt the operations of its systems.

7.2.5 Where a system is disrupted by an endpoint protection solution's operation or update, the financial institution should assess the nature and scale of the disruption to determine if the disruption is systemic or isolated. If removal of the endpoint protection solution is required, the financial institution should take appropriate action to ensure that alternative or other mitigating controls are in place to adequately secure the endpoint.

Data Loss Prevention

7.2.6 A financial institution should develop a comprehensive data loss prevention strategy to protect sensitive or confidential information. The strategy should consider how data is stored, transferred, used for operations and services, disposed, and be commensurate with the sensitivity and criticality of data.

7.2.7 Physical assets that contain or store sensitive or critical data should have appropriate safeguards in place, e.g., data encryption, strong access controls, etc.

7.2.8 A financial institution should have a process in place to identify physical assets that require more stringent encryption measures such as full disk encryption, trusted platform module, filesystem level encryption, secure enclaves, etc.

7.2.9 Staff, contractors, or third parties of a financial institution should only use authorised physical assets. Sensitive or critical data should not be stored on unauthorised physical assets and such assets should be prevented from connecting to the corporate network[11]. Measures should be in place to detect and prevent the connection of unauthorised physical assets to the corporate network.

7.2.10 Staff, contractors, or third parties should be prevented from accessing unauthorised internet services from corporate physical assets which allow the upload, download, communication, or transmission of corporate data.

Desired Outcome 7.3 – Securing Connections

General Network Security

7.3.1 A financial institution should ensure that systems are strategically allocated to network segments based on the system's criticality to the operations and services of the financial institution, and the sensitivity of the data stored or processed by the system. Network segments that host systems of high criticality or highly sensitive data should have more stringent network access controls and accompanying network security controls to mitigate against unauthorised access. A financial institution should review its network architecture regularly to identify potential security gaps and vulnerabilities arising from complexity in network interconnections.

7.3.2 A financial institution should maintain updated documentation on the network design of its IT environment, including inter-connections with external parties.

7.3.3 A financial institution should implement network access controls (NACs) to enforce security policies for users and endpoints in all network segments of the corporate network. NACs should be regularly reviewed to be kept up to date and expired or insecure policies removed promptly.

7.3.4 Firewalls, intrusion prevention solutions, and intrusion detection solutions should be installed at network perimeters to control and protect the flow of data between network segments. Such solutions can take the form of a physical device for financial institutions that operate physical infrastructure or be deployed in a cloud environment through software-based solutions.

7.3.5 A financial institution should have a process in place to evaluate connectivity options both within the enterprise and to external parties. For example, when connecting primary and secondary data centres, a financial institution may consider a dedicated leased line to provide time critical data replication stability and integrity, whereas

[11] In the context of this Guidance, corporate network refers to any and all network segments, regardless of whether the network segment is for production, development, testing, or other purposes.

connecting via application programming interfaces may be appropriate for standardised regular data downloads from a website. Depending on the type(s) and sensitivity of data transmitted, upload/download speed, resilience requirements, cost, and other factors, a financial institution should assess if connectivity between systems should be over leased lines, fixed wireless, broadband, or other means.

7.3.6 While a variety of controls are available to secure networks from threat actors, a financial institution may determine it is necessary to create an airgap for certain selected systems (i.e., ensure that such systems are available only on a separate network from other corporate systems). For such implementations, a financial institution should ensure that the means by which software or data updates are made to the air-gapped systems are done with due consideration for any control weaknesses. For example, only adequately secured and malware-free portable storage devices should be used to transfer software or data updates. A financial institution may also consider dynamic physical network segmentation that offer air-gap capabilities through logical[12] or physical[13] configurations.

Wireless Connectivity

7.3.7 Financial institutions may employ wireless access networks for various purposes and intended parties. Wireless connectivity may be offered to customers to freely browse the internet while at service centres, for staff and contractors to connect their mobile devices to the corporate network, or for Internet-of-Things (IoT) devices to transmit sensor data for analysis and reporting. However, wireless connectivity provides threat actors with a convenient entry point for malicious or criminal activity if the network is inadequately secured. A financial institution should therefore take necessary steps to secure its wireless connections and corporate devices that connect to them.

7.3.8 A financial institution should ensure that its hardware that provides wireless connectivity or devices that connect wirelessly have industry recognised certification with security features (e.g., Wi-Fi Protected Access security, Bluetooth Core Specification, radio frequency identification standards, etc.).

7.3.9 A financial institution should ensure that its wireless access networks and corporate hardware that connect to such networks are configured securely to prevent unauthorised access. A financial institution that offers free wireless connectivity to the internet for customers' or staff's personal devices should ensure that such a wireless access network is physically or logically separate from its corporate network.

7.3.10 A financial institution should implement wireless intrusion detection and prevention systems to automate scanning of rogue access points and configuration errors.

[12] For example, policy-based access controls defined at the device or user level.
[13] For example, using an out-of-band method (e.g., SMS) to notify a network segmentation device to automatically cut network traffic to defined segments.

Virtual Private Networks

7.3.11 To facilitate flexible work arrangements or to support geographically disparate offices, a financial institution may enable staff, contractors or third parties to remotely access its corporate network via a Virtual Private Network (VPN) from public networks. A financial institution should ensure that VPNs are configured securely, data is transmitted securely with end-to-end encryption, and users and devices are authenticated.

7.3.12 Financial institutions should adhere to legal requirements on the use of VPNs in the jurisdictions they operate in.

Data Transfers

7.3.13 A financial institution may implement various modes of transmitting data within the corporate network or with external systems. If inadequately configured for security, threat actors may exploit such insecure connections and compromise a financial institution's data and systems.

7.3.14 A financial institution should establish a process to ensure that all data transmission points adhere to secure transmission protocols with end-to-end encryption (e.g., SFTP, HTTPS, S/MIME, AS4, etc.). In addition to software-based encryption methods, a financial institution may consider implementing hardware-based encryption solutions to encrypt traffic between different locations.

7.3.15 A financial institution should disable all unused or unnecessary data transmission services that could be used by threat actors to compromise systems on the network, e.g., telnet, plain FTP, etc.

Securing Application Programming Interfaces

7.3.16 Application Programming Interfaces (APIs) enable systems to communicate with each other through standardised specifications. A financial institution may interact with APIs in multiple ways, including:

7.3.16.a consuming APIs from trusted third parties or untrusted public sources;

7.3.16.b publishing its own APIs for external parties to interact with its products and services; and

7.3.16.c publishing and consuming APIs for internal systems.

7.3.17 In each scenario, a financial institution should carefully assess the benefits and risks of connecting via APIs before implementation.

7.3.18 Prior to consuming APIs from external sources, a financial institution should establish a process to assess each API and the API publisher similar to the due diligence performed on sourced systems. Security characteristics of the API should also be

assessed to ensure that the communications are secured against threat actors and only requisite data can be transmitted.

7.3.19 When developing APIs for external parties' consumption, a financial institution should conduct API development in accordance with the established framework for system development and testing, and in compliance with established security configurations. Appropriate security design considerations (e.g., key management and authentication, time-delimited, data and transmission encryption, etc.) should be made depending on the expected nature of interactions with external parties (e.g., trusted closed APIs or untrusted open APIs).

7.3.20 A financial institution that publishes APIs should ensure that documentation on the use of its APIs is kept updated to the latest specifications and clearly communicates all security elements that external parties are expected to comply with in the use of its APIs.

7.3.21 A financial institution should ensure that there are no undocumented APIs[14] that threat actors could abuse to perform malicious activities in the corporate network.

7.3.22 A financial institution should log all API access activities for security monitoring and implement measures to manage traffic volume (e.g., rate limiting) and protect against malicious attacks on API connected systems. Where external parties abuse the financial institution's published APIs, a process should be in place to revoke the external parties' access promptly and securely.

7.3.23 When an API is to be retired or deprecated, a financial institution should safely decouple the API without disrupting any underlying systems or services. The financial institution should provide dependent third-parties sufficient notice of its intentions prior to retiring or deprecating the API.

Internet-Facing Systems

7.3.24 A common attack on online services (e.g., websites, transactional services, updating customer information, etc.) is the 'man-in-the-middle' (MITM) attack where a threat actor is able to eavesdrop and alter communications between parties or systems without either being aware that the connection has been compromised. While a financial institution may have robust measures in place to secure its endpoints and networks, MITM attacks can originate from external parties' (e.g., customers, third parties, etc.) devices.

7.3.25 To protect communications over the internet, a financial institution should implement secure transmission protocols (e.g., TLS, certificate pinning, etc.) to encrypt communications between its systems and connecting parties. Each secure

[14] Undocumented or shadow APIs are not meant for use by end users but instead serve as code that developers may use for troubleshooting or automating functionalities.

communication should be time-delimited through stateful session management, with re-authentication required upon session expiry.

7.3.26 Financial institutions should implement web application firewalls that analyse and protect against malicious web-based traffic (e.g., SQL injection, cross-site scripting, etc.).

7.3.27 A financial institution should implement measures to prevent web parameter pollution attacks that exploit the logic of the web application. Sensitive data should not be in the clear in the URL, HTTP data, and cookies, and secure programming techniques should be applied to ensure that only expected data is accepted by the web application.

7.3.28 A financial institution should implement measures (e.g., multi-factor authentication, CAPTCHA[15], hidden fields honeypot, image identification, user interaction, etc.) to detect and mitigate tools used by threat actors to target web addresses and parameter values. Such tools enable threat actors to overload a financial institution's computing resources, extract content for reselling, or even to reverse engineer the website to make customer phishing scams more effective.

7.3.29 Another common attack on internet-facing systems is a 'Denial-of-Service' (DoS) attack where a threat actor attempts to make a system unavailable by flooding the intended target with requests thereby overloading the system or preventing the fulfilment of legitimate requests. Motivated threat actors may leverage on multitudes of computer resources to perform a 'Distributed DoS' (DDoS) which is significantly harder to mitigate against as blocking a single source would be insufficient.

7.3.30 A financial institution should monitor network traffic to its internet facing systems to detect sudden surges in system resource utilisation and a process in place to activate anti-DoS or anti-DDoS mitigation measures when necessary.

7.3.31 Given the growing scale at which DDoS attacks occur, a financial institution may engage internet service providers or other vendors that provide scalable anti-DDoS services such as content filtering or scrubbing, blackholing, content delivery networks, etc, to deal with the veracity of DDoS attacks. Prior to engagement, the financial institution should perform a comprehensive assessment to evaluate the types of DDoS mitigated, mitigation measures offered, promptness and scale of protection offered, and adequacy of reporting of the potential service provider.

7.3.32 A financial institution should ensure that its online and mobile services are provided through secure and official channels. Mobile applications should be offered for download via official mobile platform stores (e.g., Google Play Store, Apple App Store, etc.), and internet-based financial services should be hosted on domains that are under

[15] A Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a tool to ascertain if input has not been generated by a computer.

the financial institution's control and are well-managed for security (e.g., DNSSEC[16], TLS certificates, etc.) and availability (e.g., renewal, troubleshooting DNS issues etc.).

7.3.33 Mobile applications developed by the financial institution should adhere to the financial institution's established framework for system development and testing, and configured to established standards.

7.3.34 A financial institution should ensure that its customer-facing mobile applications are tamper resistant or have appropriate controls in place to restrict transactional activity in the event the customer's mobile device is compromised.

7.3.35 A financial institution should protect its domain(s) from abuse by threat actors who exploit email protocols to conduct scams. Solutions that enable email authentication (e.g., SPF, DKIM, DMARC[17]) to mitigate against email spoofing attacks (e.g., business email compromise, spear phishing, domain spoofing, etc.) should be implemented or adopted.

Desired Outcome 7.4 – Securing the Virtual Environment

7.4.1 While securing individual physical assets and the connections they have to the corporate network creates layers of defence against threat actors, the virtual environments in which a financial institution operates in also requires attention and action.

Corporate Virtual Machine and Mobile Environments

7.4.2 Access to the corporate network or to corporate data may take place through corporate issued devices or through non-corporate issued devices that connect to the corporate network through secure channels. Commonly known as 'Bring-Your-Own-Device' (BYOD), facilitating non-corporate issued devices access to corporate resources has productivity and cost benefits for a financial institution, but also presents risks as such devices may have varied security postures and will expand the attack surface for threat actors. A financial institution that allows staff, contractors and third parties to use non-corporate issued devices to connect to the corporate network should implement measures to prevent unauthorised access and data loss.

7.4.3 Virtual machines allow financial institutions to quickly provide numerous virtual environments that are accessible from any connected device. A financial institution should establish processes to govern the lifecycle of virtual machines and ensure that they are configured to established standards and regularly updated. Processes should also be in place to ensure that data in virtual machines are securely stored and protected from unauthorised access or compromise. Where applicable, the financial

[16] Domain Name System Security Extensions (DNSSEC) strengthens authentication in DNS using digital signatures based on public key cryptography. It comprises a suite of extension specifications by the Internet Engineering Task Force for securing data exchanged in the Domain Name System in Internet Protocol networks.

[17] Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are methods to detect forged sender addresses while Domain-based Message Authentication, Reporting and Conformance (DMARC) enables domain owners to protect their domain from unauthorised use.

institution should implement controls or adopt virtualisation software that can prevent data loss from the connecting physical device's memory e.g., memory encryption.

7.4.4 A financial institution that enables its staff, contractors and third parties to interact with the corporate environment or access corporate data via mobile applications should adopt solutions that securely govern the access and use of corporate resources.

7.4.5 Where possible, a financial institution should implement capabilities that ascertain the security posture of the non-corporate issued device prior to providing access to corporate resources. Devices that fail the security posture assessment (e.g., not updated to latest software version, jailbroken or rooted mobile devices, malware infected devices, etc.) should be denied access unless the virtual machine or mobile application has robust security measures that insulates corporate resources effectively to prevent compromise. In the event the non-corporate device is lost or stolen, the financial institution should be able to remotely wipe any corporate data.

7.4.6 A financial institution should enforce strict security policies on the transmission of data or programs into and out of virtual machines or mobile applications to prevent threat actors from inserting malware or extracting data for exploitation.

Web Services for Automation and Collaboration

7.4.7 There are innumerable work automation and collaboration services available over the internet that financial institutions could subscribe to and avoid investing in developing their own solutions or purchasing products to be run on corporate infrastructure. While cost efficient and accessible from any internet connected device, a financial institution should be aware of the confidentiality, integrity, and availability risks associated with such services.

7.4.8 A financial institution should perform due diligence on the web service's track record, service standards, resilience arrangements, alignment with required business need, and past reported incidents of unavailability or data compromise. Approval from an appropriate level of management within the financial institution should be sought prior to use of the web service.

7.4.9 If a financial institution adopts commercial mobile applications for work productivity or collaboration purposes, due diligence on the vendor and its product's security posture should be performed to ensure that corporate resources accessed by the mobile application are not at risk.

Desired Outcome 7.5 – Updating the Environment

7.5.1 A financial institution may have separate IT environments for development activities, testing prior to deployment, and a live environment containing production systems supporting business functions. Access to each environment should be strictly controlled on a needs-basis and any interaction between environments should be stringently monitored to prevent unauthorised activities, contamination of data, or infections from malware.

7.5.2 Where data from the production system is required for use in non-production environments for testing or development activities, steps should be taken to obtain appropriate approvals, mitigation measures in place to ensure personal data protection, and strict access controls in place to stringently manage the data transfer process to prevent data leakage.

Change Management

7.5.3 A financial institution should establish a change management process to ensure that IT assets are not altered without oversight or in a way that disrupts business operations or services to customers. Changes can take the form of IT projects to improve a system, technology refresh, configuration updates, patches, etc. The change management process should include, among other elements, assessments of the proposed changes to determine the business need, urgency of the change, risks mitigated or created by the change, performance impact of the change, and any impact to connected systems.

7.5.4 A financial institution should ensure that changes comprising firmware or software releases from third parties should be acquired only from verified sources. Where applicable, the acquired change should be validated by confirming an identical checksum with the vendor published release information.

7.5.5 All changes to systems should be approved by an appropriate level of management within the financial institution.

7.5.6 Where a change requires expedited action to mitigate a time-critical issue, a procedure should be in place to ensure that appropriate steps are taken to address the issue with a commensurate delegation-of-authority.

Patch Management

7.5.7 As part of the change management process, a financial institution should establish a patch management process to ensure that all its firmware[18] and software are kept up to date with the latest fixes for defects, and vulnerabilities. The process should include, among other elements, an assessment on the criticality[19] of the patches and the software or firmware the patch is to be applied to, and a timeframe for patch implementation that is commensurate with business need and the risks addressed by the patch.

7.5.8 A financial institution should ensure that it acquires patches only from verified sources and validates the integrity of the patch. Where applicable, the acquired patch should be validated by confirming an identical checksum with the vendor published patch information.

[18] Firmware is software that provides basic machine instructions that enables the hardware to function and communicate with other software running on a device.
[19] For security vulnerabilities, financial institutions may take reference from the Common Vulnerability Scoring System (CVSS) which provides a numerical score that enables prioritisation by severity.

7.5.9 While virtual patching[20] enables timely mitigation of known vulnerabilities, financial institution should not treat virtual patches as permanent solutions. Financial institutions should regularly review the list of virtual patches with the aim of implementing the requisite updates to the applications in a timely manner.

Testing

7.5.10 All changes and patches[21] should be tested in a separate test or development environment prior to being applied. Testing enables the financial institution to ensure that the updated system is still compatible with connected systems and identify any performance issues or disruptions resulting from the change or patch.

7.5.11 Testing should include relevant stakeholders (e.g., business users, IT staff, etc.), with clearly defined test scenarios and desired test outcomes. All test results and stakeholder acceptance should be documented.

Deployment to Production Environment

7.5.12 A financial institution should ensure that only authorised staff are able to deploy changes or patches into the production environment. Such authorised staff should be competent, familiar with the financial institution's systems, and empowered with strictly controlled access rights to production systems. Where the change or patch requires movement of source code or binaries, the financial institution should be able to ascertain the author of such movement and ensure that measures are in place to check and maintain the integrity of source code moving between IT environments.

7.5.13 Prior to deployment, backups of the system(s) to be changed or patched should be performed, enabling the financial institution to have a point-in-time instance of the system, its configurations, and data.

7.5.14 During deployment, the financial institution should monitor the system(s) to ensure correct functioning and to identify any issues that may arise. Information generated by logs should be captured to facilitate such monitoring and any potential troubleshooting or investigations should the change or patch encounter issues.

7.5.15 Financial institutions should also establish rollback procedures to cater for unexpected failures during the process of implementing a change or patch in the production environment. Such rollback procedures should include system-specific steps taken to revert the patched or changed system to a previous state.

[20] Also known as 'external patching' or 'just-in-time patching', virtual patching creates a security policy enforcement layer which prevents the exploitation of a known vulnerability. The actual source code of the application is not modified.

[21] There are certain types of patches that may not need to be tested where the potential risks associated with such patches may be low. For example, patches provided by the software or firmware vendor designed to fix minor issues that are not critical to the operation of the system. Nonetheless, financial institutions should have a process in place to identify such patches and the appropriate activities for deployment.

7.5.16 Where blue-green[22] deployment strategies are adopted, financial institutions should ensure that the strategy is appropriate for change or patch, and the complexity of the systems, and that all system dependencies, including data schemas are fully mapped prior to implementation.

7.5.17 A financial institution that relies on third parties to update its systems should have procedures or controls in place to be informed of activities performed in the production environment. Where necessary, depending on the criticality of the system, the financial institution should obtain assurance on the third parties' activities in the production environment by engaging appropriate independent parties to review the changes performed.

[22] A blue-green deployment model is one where two separate sets of resources are running in parallel, and traffic is gradually directed from one set to another as the resources on the latter set is updated following a change release.

Desired Outcomes for Data Lifecycle Management

Desired Outcome 8.1 – Data Governance: A financial institution should have organisational structures to support sound governance of data.

Desired Outcome 8.2 – Data Lifecycle Management: A financial institution should safely and securely manage its data from inception to destruction.

Desired Outcome 8.3 – Handling Data with Regulatory Obligations: A financial institution should ensure it complies with all applicable regulatory obligations pertaining to its data.

Desired Outcome 8.1 – Data Governance

8.1.1 As a financial institution grows and expands its suite of services, so too does the universe of data that it manages and the potential for data related risk events (e.g., data leakage, etc.).

8.1.2 To adequately govern such growing data sets, a financial institution should put structures or mechanisms in place that enables it to maintain oversight and control. For example, this may take the form of formalised policies on data governance, a dedicated function and appointed senior executive to oversee data governance for the financial institution, or a cross-functional data governance committee charged with a data governance mandate. Such structures or mechanisms should be integrated within the financial institution's risk management framework.

8.1.3 The governance framework should include assigning accountability for each dataset to an appropriate and responsible senior executive to ensure that the dataset is managed in line with the established data governance policies (e.g., granting of access rights to the data sets across different systems and business activities).

8.1.4 A financial institution should ensure that it has appointed competent and responsible staff to manage its datasets in line with its data governance policies. The responsibilities of these staff should include overseeing the day-to-day consumption of the dataset and managing the technical aspects relating to data lifecycle management (e.g., security controls for storage, processing, etc.).

8.1.5 A financial institution should put processes in place to ensure that any deviations from the data governance framework are approved by the appropriate level of management and that any necessary actions to mitigate the risks of the deviation have been identified and taken. The financial institution should regularly review approved deviations to ensure that the associated risks are still adequately managed.

Desired Outcome 8.2 – Data Lifecycle Management

8.2.1 A financial institution can collect and generate tremendous volumes of data which are necessary for operations, services, and business decisions. The variety of data

generated and collected include, among other types, customer data (e.g., Know-Your-Customer (KYC) information, etc.), transaction data (e.g., payment information, billing, fees, etc.), corporate data (e.g., internal communications, minutes of meetings, approval documents, payroll information, intellectual property, reporting, etc.), or technical data (e.g., network diagrams, source code documentation, logs, etc.). Some data sets, such as personally identifiable information, are sufficiently sensitive to have regulatory obligations on how it is obtained, processed, stored, and retained. A firm understanding of the data lifecycle will enable financial institutions to effectively and efficiently manage data to achieve its desired outcomes and comply with regulatory obligations.

8.2.2 A financial institution should establish a data lifecycle management framework that sets out the policies and procedures on data management for each stage and the roles and responsibilities of staff when dealing with data at each stage.

Data Generation and Collection

8.2.3 Data can be acquired through various means. Data is generated for various purposes when systems interact with each other or with users. Data is collected when customers or external parties submit information through forms, email or make payments. Data can also be generated through logging of system or user activities. These and other acquisition methods result in structured or unstructured data formats that require different approaches for capture.

8.2.4 A financial institution should have a process in place to identify the various datasets it generates and collects, and assign accountability. For example, identification can take place at suitable junctures such as during system development, upon finalisation of third-party arrangements, or when business units interact with technology teams to design data collection mechanisms.

8.2.5 A financial institution should have a mechanism to inventory its various datasets. Such an inventory should detail the type, form, acquisition channel, who has access to the data, location of data, whether data is held internally or by a third party, and other elements necessary for a financial institution to have oversight of the variety and volume of data it generates and collects.

8.2.6 On a regular basis, a financial institution should review its inventory of datasets to determine if acquired data is still necessary, of adequate quality, unnecessarily duplicated, or can be acquired in more effective or efficient ways.

8.2.7 For all data generated by the financial institution, measures should be put in place to minimise excessive generation of sensitive data. For example, as part of the software development framework, data presented in logs should be designed to minimise the likelihood of unauthorised users inadvertently having access to sensitive data, e.g., customer personal information, payroll data, etc.

8.2.8 Similarly, when collecting or acquiring data, a financial institution should only collect the scope of data necessary to achieve its objectives and minimise where possible any collection of sensitive data e.g., personal data.

Data Processing

8.2.9 Processing of data can take place in structured system processes or through user interaction. It can also vary in purpose such as cleaning and transforming raw data into more accessible or usable data, ingesting data as input for business processes, tokenising data to mask sensitive information, or encrypting data to protect against unauthorised access.

8.2.10 A financial institution should ensure that its system development practices are disciplined to only make use of necessary data to achieve established objectives, and that relevant privacy or privilege protections are maintained throughout the development process.

8.2.11 When designing systems for data processing activities, financial institutions should ensure that systems are adequately resourced to meet processing performance requirements and would not result in disruption to business operations or services to customers.

Data Classification

8.2.12 A financial institution should establish policies and procedures to classify all collected, generated, and processed data according to the sensitivity and criticality of each dataset.

8.2.13 Depending on the classification of data, appropriate controls should be implemented in accordance with the sensitivity or criticality of the data. For example, confidential data such as customer personal information should be encrypted in storage, use and in transit, and protected with strong access controls.

8.2.14 A financial institution should regularly review its data classification policies and the assigned classifications to its datasets to ensure that the classification remains relevant and aligned with the financial institution's risk management framework.

Data Storage and Archival

8.2.15 Data can be stored in a variety of formats, mediums, and states. There are many technologies available to facilitate storage with mechanisms for high availability, low latency, scalability, networked access, security, and energy efficiencies.

8.2.16 A financial institution should establish a system and data storage framework that both meets business needs and contributes fully to its operational resilience. The framework's policies and procedures should pertain to both operational and backup storage. The framework should prescribe the manner in which various data sets are stored, security controls appropriate for respective data classifications, frequency of

operational and backup storage activities, retention period, archival, and restoration testing procedures.

8.2.17 All storage systems and media should be configured in adherence to established configuration standards and kept up to date to address security vulnerabilities or apply system enhancements.

8.2.18 A financial institution should establish risk-appropriate data storage procedures and controls (e.g., encryption, masking, etc.) for its various environments (e.g., development, test, production, etc.) at the system, database, and application levels.

8.2.19 Where high availability capabilities are required, a financial institution should ensure that the data storage implementation has capabilities to mitigate against data corruption, or single points of failure.

8.2.20 A financial institution should segregate archived data that is no longer required for ongoing business operations to prevent mixing or mishandling. Archived data may be stored in long-term storage systems (e.g., tape storage, cloud, etc.) for future use (e.g., compliance, audit, investigation, etc.).

8.2.21 A financial institution should conduct and document regular restoration tests to ensure that its data stored in backup is recoverable and that staff are familiar with restoration procedures.

Data Usage, Transfer, and Sharing

8.2.22 Without adequate controls and protections, financial institutions may find data inappropriately traversing between repositories, business functions, or even to external parties, and potentially expose the financial institution to a breach of its regulatory obligations.

8.2.23 A financial institution should establish policies and procedures on the use and transfer of classified data, as well as for the sharing of data with internal and external parties (e.g., data aggregators, regulators and authorities, etc.).

8.2.24 A financial institution should ensure that staff abide by acceptable use policies for the use of data. Staff of a financial institution should ensure that appropriate permissions and access controls are applied for each system used, including collaboration tools that facilitate work on classified data.

8.2.25 A financial institution should ensure that appropriate security controls are applied when transmitting classified data internally or externally. For example, when sending classified data to external parties, secure methods of file transfer should be used to prevent interception and unauthorised access to data by threat actors.

Data Destruction

8.2.26 A financial institution should establish policies and procedures to govern the safe, secure and timely destruction of its data both internally as well as relevant data in possession of its third parties.

8.2.27 A financial institution should maintain a record of data destroyed and ensure that its asset inventory is updated in a timely manner when data and its associated storage media is destroyed.

Desired Outcome 8.3 – Handling Data with Regulatory Obligations

8.3.1 A financial institution should be mindful of datasets that come with regulatory obligations (e.g., statutory record-keeping, personal data, etc.) and design acquisition mechanisms to be built with compliance from the onset.

8.3.2 A financial institution should be able to quickly locate and manage data that fall under regulatory obligations.

8.3.3 A financial institution should implement controls that would enable compliance with regulatory obligations (e.g., time-bound data retention, etc).

8.3.4 Financial institutions should be clear of their reporting obligations when a risk event impacts data that have regulatory obligations and report to the relevant authorities in a timely manner e.g., data breach incident involving personal data.

Desired Outcomes for Resilience

Desired Outcome 9.1 – Availability Architecture: A financial institution should architect its systems, networks, and data to meet its availability objectives.

Desired Outcome 9.2 – Continuity Planning: A financial institution should have business continuity plans in place to minimise the impact of disruptions on its ability to deliver financial services.

Desired Outcome 9.3 – Recovery Planning and Testing: A financial institution should recover from disruptions promptly and safely.

Desired Outcome 9.1 – Availability Architecture

9.1.1 A financial institution should establish availability objectives for its operations and services to customers. This can be derived from service level expectations the financial institution commits to customers or from regulatory requirements on the provision of regulated financial activities.

9.1.2 A financial institution should regularly conduct reviews of its systems, networks, and data architecture to identify and remove design weaknesses and single-points-of-failure (SPOF). The review should include a mapping of dependencies within the financial institution's IT environment as well as dependencies on external parties (e.g., group or related entities, technology vendors, APIs, etc.).

9.1.3 Concentration risk in the technology context can arise from multiple contexts. At the industry level, certain third parties' products or services may be preferred over others resulting in a concentration of financial institutions relying on a small group or a single third party for products or services. Some financial institutions are part of a group structure with multiple entities globally relying on a single entity in the group for outsourced services. Within a financial institution, concentration risk can arise when all of its systems are provided by a single service provider or located in a single data centre. Akin to the removal of SPOFs, a financial institution should endeavour to reduce the potential for concentration risk or adopt measures to mitigate the risk.

Systems Resilience

9.1.4 While a financial institution may implement various security measures to protect against a range of risk events, architecting its systems, networks and data to achieve high availability is also key to effective IT risk management. Non-malicious risk events, such as product launches that spur a sudden increase in customer visits to online services resulting in slow or overwhelmed servers, can also impact a financial institution's reputation and require forward planning to prevent recurrence.

9.1.5 When designing its systems, a financial institution should incorporate considerations that optimise utilisation of resources and reduce bottlenecks in performance. Where

high availability is required or for critical system components/services, a financial institution should implement redundancy and/or fault tolerant solutions.

9.1.6 A financial institution should ensure that its hardware and software are adequately provisioned to support its operations. Indicators for system performance, utilisation, and capacity should be monitored and procedures should be in place to respond promptly and safely when pre-defined thresholds are met e.g., allocating additional capacity for anticipated service demand surges, etc.

9.1.7 A financial institution should adequately communicate expectations of availability under normal or stressed circumstances to stakeholders. For stressed circumstances, drawer plans should be in place to clearly indicate if the system or service is experiencing greater than anticipated demand on availability or is disrupted.

Network Resilience

9.1.8 To facilitate high availability, a financial institution should implement network redundancy measures within its IT environment (e.g., switches, routers, etc.) that create multiple paths to systems and route traffic effectively (e.g., load balancing) to maximise utilisation of resources and eliminate SPOFs.

9.1.9 Terrestrial and undersea telecommunications networks are deeply interconnected and rely on shared resources such as exchanges where internet service providers exchange and route data. If disruptions were to occur at such shared resources or other points of routing coalescence, a financial institution's operations and service to customers may be disrupted.

9.1.10 A financial institution should conduct a telecommunications diversity assessment to determine the extent of network redundancy necessary for its operations and services to customers. The assessment should include connections between the financial institution's data centres, connections to the internet for critical systems, and connections to third parties that play a critical role in the financial institution's operations and/or service to customers.

Data Centre Resilience

9.1.11 There are a variety of hosting options for financial institutions. A financial institution may have a server room on its premises or build and operate its own data centre. A financial institution may lease infrastructure in managed data centres or choose co-locating in data centres run by third parties. Cloud service providers also offer a range of services that financial institutions can choose from, each with varying degrees of responsibilities and choice of geographic locations.

9.1.12 A financial institution should make an assessment of the available options to determine which model meets its business needs, risk appetite, and regulatory requirements. The assessment should also include a Threat and Vulnerability Risk Assessment (TVRA) to evaluate the data centre's protections against physical and environmental threats. Given the reliance on public infrastructure needed to operate a data centre (e.g.,

telecommunications, power, and water supply, etc.), the political and economic climate of the country the data centre is located in should be factored into the assessment. As and when material changes in the threat landscape occur, the financial institution should review its assessment and take appropriate action where necessary.

9.1.13 To strengthen availability to systems and data, a financial institution should implement redundant data centres to serve as secondary or disaster recovery data centres. Appropriate availability models should be adopted (e.g., active-active, active-passive, hot/warm/cold storage, masterless clustering, etc.) depending on the objectives set out by the financial institution. The redundant data centre(s) should be geographically separated from the primary data centre and relying on different set(s) of physical infrastructure providers (telecommunications, utilities, etc.) to mitigate against risk events that impact the underlying infrastructure.

9.1.14 A financial institution should assess the environmental and redundancy arrangements for individual data centre infrastructure (e.g., telecommunications, power and water supply, cooling systems, fire suppression, temperature, and humidity control systems, etc.) to ensure that SPOFs are eliminated where feasible.

9.1.15 A financial institution should ensure that the data centre's physical security, upkeep and maintenance, and environmental controls are monitored on an ongoing basis with established and tested procedures to escalate and respond to any risk events.

9.1.16 A financial institution should ensure that access to the data centre is strictly controlled with comprehensive physical and logical controls to manage and monitor access from entry to the data centre to accessing the equipment racks holding the financial institution's data.

Desired Outcome 9.2 – Continuity Planning

9.2.1 Without adequate planning to ensure business continuity during disruptions, a financial institution is at risk of incurring financial losses, regulatory action, and losing the trust and confidence of its customers and counterparties in the financial ecosystem.

9.2.2 To appropriately prioritise systems for recovery during a disruption, a financial institution should establish a business continuity framework for the identification of critical business services and functions as well as roles and responsibilities during a crisis. Among other factors, the framework should consider the impact on the financial institution's viability, customers, and interconnections in the financial ecosystem when each business service or function is unavailable (e.g., business impact analysis). Dependencies and/or interconnections across a financial institution's business services and functions should also be considered. Third parties involved in the operation or delivery of a business service or function should be included in the criticality analysis.

9.2.3 The business continuity framework should define for each business service or function minimum acceptable service levels which would serve as trigger points for the activation of business continuity measures. This will enable a financial institution to

proactively address operational disruptions before complete service or function degradation.

9.2.4 The framework should also include the maximum disruption duration that the financial institution is able to tolerate for each business service or function. This will inform the recovery time objectives (RTO) to be set for systems supporting each business service or function.

9.2.5 A financial institution can then prioritise systems that support the most critical business services and functions, and/or systems that have the shortest RTOs for recovery. Prioritisation should take into consideration the resources available and any regulatory obligations on system recovery during disruptions.

9.2.6 In addition to RTOs, a financial institution should also establish recovery point objectives (RPO) for data recovery efforts. Once established, RPOs should be propagated to the financial institution's data lifecycle framework.

9.2.7 With the system recovery prioritisation, a financial institution should establish its IT business continuity plans (BCP). The IT BCP should include protocols for activation and escalation, roles and responsibilities of relevant personnel involved, and metrics for monitoring of recovery activities.

9.2.8 A financial institution should identify the relevant personnel with appropriate seniority and expertise to constitute a steering group to lead the financial institution's response to a disruption and to ensure that both internal and external stakeholders are kept apprised of activities occurring during activation of business continuity measures. Procedures should be established to convene the steering group when defined disruption thresholds are met.

Desired Outcome 9.3 – Recovery Planning and Testing

9.3.1 While it is not possible to account for every possible disruption scenario, setting out recovery plans assists in building a firm understanding of what is within the financial institution's control during a disruption and the actions that can be taken to deal with disruptions.

9.3.2 In developing a recovery plan, a financial institution should study a range of scenarios and identify what disruptions would result from each scenario. For example, a faulty hardware could result in system failure thereby disrupting business operations or services to customers. The exhaustiveness of the scenario analysis should be in relation to the scale and complexity of the financial institution's IT environment and dependencies.

9.3.3 A financial institution should establish recovery plans in line with the established RTOs and RPOs arising from the business continuity framework. Recovery plans for all systems should be sufficiently detailed to prevent unauthorised or inappropriate activities from being performed. A financial institution should ensure that its recovery plans are approved by the appropriate level of management.

9.3.4 On a regular basis, the recovery plan should be reviewed and updated to account for changes made to the IT environment and dependencies, and changes to other policies and procedures that have an impact on recovery activities.

9.3.5 A financial institution should also remind its staff that use EUC resources to make alternative arrangements or work with the relevant functions to include EUC resources into the business continuity plans to facilitate seamless business operations during recovery activities.

9.3.6 A financial institution should regularly test its recovery plans to validate its ability to recover from disruptions in a timely and safe manner. Relevant stakeholders, including senior management and business units, should participate in such tests to gain competence in the necessary activities. Third parties that operate or deliver a business service or function should be involved in recovery tests or facilitate the financial institution's participation in their recovery tests.

9.3.7 Where possible, a financial institution should regularly operate fully from its recovery or alternative arrangements to build confidence that such infrastructure is in working order and its personnel are accustomed to performing the necessary activities during BCP activation.

9.3.8 Upon activation of the IT BCP, a financial institution should ensure that recovery activities adhere to the rehearsed, tested, and approved procedures. Where deviation is necessary due to unforeseen circumstances, appropriate personnel should perform adequate risk assessment of the deviation and obtain approval from the appropriate level of management prior to execution.

Desired Outcomes for Cyber Event Management

Desired Outcome 10.1 – Threat Awareness: A financial institution should stay apprised of the latest cyber threats to its IT environment.

Desired Outcome 10.2 – Cyber Event Lifecycle Management: A financial institution should ensure cyber events are managed to resolution promptly and safely.

Desired Outcome 10.3 – Security Testing: A financial institution should validate its ability to prevent, detect, and be resilient against cyber threats.

Desired Outcome 10.1 – Threat Awareness

10.1.1 While financial institutions strengthen their defences by implementing robust controls to mitigate IT risks, threat actors are also improving their toolkits to find the next exploit. Staying up to date with developments in the cyber threat landscape is essential to ensuring that a financial institution's IT environment is not at risk of falling victim to known threats.

10.1.2 A financial institution should maintain an awareness of developments in the cyber threat landscape that would inform the enhancements to be made to its security controls. For example, adjusting DDoS mitigation measures to align with known attack volumes, updating anti malware signatures to ensure new ransomware variants are detected and mitigated, or replacing software or hardware when fundamental vulnerabilities are discovered. Sources of such cyber threat information include openly available knowledge bases of known vulnerabilities[23] and attack methods[24], as well as alerts and advisories published by various national cyber security centres.

10.1.3 Cyber threat awareness building can be done in-house by establishing a threat intelligence function or through engagement of third parties that provide cyber threat intelligence monitoring services. Such a function or service may also gather information pertaining to abuse of the financial institution's intellectual property (e.g., logos, website impersonation, etc.) or data (e.g., exfiltrated customer or corporate information) and take active steps to halt continued abuse such as engaging the abuser's internet service provider to submit a takedown request.

10.1.4 A financial institution should establish policies and procedures for the appropriate classification[25] and dissemination of intelligence. Sharing of the gathered intelligence

[23] The Common Vulnerabilities and Exposures (CVE) program aims to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.
The Open Web Application Security Project (OWASP) Top 10 provides the top 10 critical security risks to web applications based on broad consensus of security experts globally.
[24] The MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.
[25] A common classifying system is the Traffic Light Protocol (TLP) which defines how widely information should be circulated according to specific colours of a traffic light.

and the assessment of the impact of such intelligence on the financial institution should be done in a controlled manner to prevent actionable intelligence falling into the hands of threat actors.

10.1.5 A financial institution should also maintain an awareness of known threats to its third parties. Where the gathered intelligence highlights or points to potential concerns about a third party' ability to mitigate a threat, the financial institution should engage the third-party and obtain assurance that the third-party has the requisite controls in place to mitigate the threat.

10.1.6 As threat information benefits from an active community of participants, financial institutions are encouraged to contribute to cyber threat information sharing initiatives and participate in cyber threat information sharing arrangements.

Desired Outcome 10.2 – Cyber Event Lifecycle Management

10.2.1 Aside from incidents that cause disruptions to business operations or services to customers, a financial institution should also be able to promptly and safely manage cyber events that may result in system or data compromise leading to financial, reputational or legal risk events.

10.2.2 A financial institution should implement solutions that collect, aggregate and analyse logs and other data sources to detect cyber events[26] – activities occurring in the IT environment that could result in or contribute to incidents – and take prompt action to address such cyber events. Such solutions should be configured to monitor unexpected and anomalous changes, behaviour or activities by users, systems, processes and services throughout the financial institution's systems and networks and at entry/exit points of the network perimeter. A financial institution should regularly review the rules/configurations of such solutions to ensure their effectiveness in detecting new known threats and update them in a timely manner.

10.2.3 To facilitate prompt action in addressing cyber events, a financial institution should establish procedures to respond to cyber events of various natures. Such procedures should include classification of cyber events by severity, technical activities for issue resolution, escalation protocols and reporting, and integration into the financial institution's incident management framework and business continuity plan where appropriate.

10.2.4 On an ongoing basis, a financial institution should ensure its monitoring solution(s) stays updated to account for evolved or new threats, including scanning its IT environment for indicators of compromise as they become available.

[26] For example, Security Information and Event Management (SIEM) solutions facilitate the detection of potential threats and vulnerabilities. Security Orchestration, Automation and Response (SOAR) solutions can also assist in automating detection and response workflows.

10.2.5 A financial institution that engages a third party to provide cyber event management services[27] should perform adequate due diligence on the third party and have ongoing oversight over the performance of the service. The financial institution should have visibility into the monitoring rules and escalation protocols employed by the third party specific to the financial institution, as well as regular reporting from the third party on cyber event case management. The financial institution should integrate the third party's cyber event response into its incident management framework.

Desired Outcome 10.3 – Security Testing

10.3.1 A financial institution should validate the effectiveness of IT controls. Baseline validation can take the form of vulnerability assessments while more advanced validation can be obtained by adversarial forms of testing.

10.3.2 A financial institution should establish a process to conduct vulnerability assessments (e.g., identifying configuration errors, insecure design, outdated anti-virus signature library, etc.) of its IT environment both on a regular basis and as relevant cyber threat information comes to light. Critical systems should be prioritised for assessment and findings from the vulnerability assessments should be addressed in accordance with the financial institution's change and patch management processes. Such assessments can take reference from common industry standards or from vendor recommendations for security configurations.

10.3.3 A financial institution should regularly arrange for adversarial types of testing on its production systems and networks with adequate safeguards. Such testing can take the form of traditional penetration tests of online platforms, social engineering exercises such as phishing email campaigns on staff, threat hunting exercises, bug bounty programmes where ethical hackers are incentivised to report vulnerabilities to the financial institution, or red teaming exercises where a team of cyber security experts are permitted to simulate sophisticated threat intelligence-driven targeted attacks against the financial institution. Findings arising from these adversarial tests should inform remediations or enhancements to controls in the financial institutions IT environment as well as improvements to policies, procedures, and processes where a technical control cannot be implemented.

10.3.4 In determining the scope of adversarial testing, the financial institution should consider the following:

10.3.4.a A review should be conducted to identify what assets should be tested and the objectives to be achieved from testing those assets.

10.3.4.b Based on the identified assets, scenarios of compromise should be defined based on the channels through which a threat actor could reach the assets[28].

[27] These are typically provided via managed security operation centres that offer a suite of monitoring, protection, detection, and incident response services.
[28] With the scenarios of compromise identified, a financial institution can take steps to then define countermeasures to prevent, or mitigate the effects of, threats to the asset as part of a threat modelling exercise.

10.3.4.c The approach and methodology of the test should be defined. The approach could take the form of the examples listed in 10.14 or other types of test approaches which are outcome-based (e.g., capture-the-flag[29]). Where applicable, the testing methodology should include an agreed 'stop point' which can be used a criterion to evaluate the results of the test (e.g., compromising privileged account credentials, performing privilege escalation, etc.). The stop point is crucial in containing the potential harm that may arise from the testing party's infiltration activities.

10.3.4.d Appropriate tools should be chosen to perform the test in accordance with the test objectives, approach, and methodology.

10.3.4.e An appropriate duration should be set commensurate with the test objectives, approach, and methodology. If such tests are performed on the production environment, the tests should not compromise the delivery of financial services to customers e.g., scheduling such tests outside of peak usage periods.

10.3.4.f All findings should be formally documented and prioritised according to the severity, impact, and likelihood of the identified vulnerabilities. Where appropriate, the financial institution should establish or adopt a risk rating methodology[30] that would enable a standardised approach to classifying vulnerabilities relevant to their business impact on the financial institution. The financial institution should remediate all findings and retest them to validate the effectiveness of remediation prior to closure of the finding.

10.3.5 Where appropriate and depending on the nature and objectives of the test or exercise, a financial institution should involve relevant stakeholders, such as the governing body, senior management, business functions, third party service provides and customers.

[29] Capture-the-flag exercises involve ethical or white hat hackers who are given a specific target within an organisation's IT infrastructure to 'compromise'. The hackers can use any tools and exploit any channel to reach the target within a time frame.

[30] For example, the OWASP Risk Rating Methodology espouses six steps to estimate the severity of risks to the business and make informed decisions about mitigating those risks.

SECTION C: INTERACTING SECURELY

Chapter 11 – Access Management

Desired Outcomes for Access Management

Desired Outcome 11.1 – Credential Management: A financial institution should ensure that credentials used to access its assets and networks are valid.

Desired Outcome 11.2 – Authorisation: A financial institution should ensure that access to its assets is managed and authorised on a least-privileged basis.

Desired Outcome 11.3 – Authentication: A financial institution should only allow access to its assets, appropriate to the authorised scope of activities, upon successful authentication of credentials.

11.0.1 As financial institutions adopt more systems and expand their technology infrastructure, it is inevitable that the task of mapping and managing access to resources will become more complex. In this growing complexity, it is essential that financial institutions implement robust controls for identity and access management to mitigate against the threat of unauthorised access.

11.0.2 A financial institution should establish an identity and access management framework encompassing policies and procedures for credential management, authorisation (assigning rights to a credential), and authentication (verifying a credential).

Desired Outcome 11.1 – Credential Management

11.1.1 Credentials are pieces of information that serve as identities in the digital world and facilitate authorisation and authentication of users and systems. Credentials can take various forms e.g., usernames and passwords, certificates, tokens, and cryptographic keys, etc.

11.1.2 As part of its identity and access management framework, a financial institution should establish procedures for the management of credentials throughout its lifecycle. Processes and procedures should also be in place to revoke and replace credentials that have been compromised. All credential requests should be approved by the resource owner and appropriate level of management.

11.1.3 Depending on the type of credential to be employed, a financial institution should implement appropriate solutions to securely issue, modify, and revoke credentials. Where credentials are stored within a solution, the financial institution should ensure that credentials are stored securely (e.g., encryption at rest) commensurate to the assigned access rights of the credential. Similarly, access to such credential storage solutions should be securely controlled (e.g., multi-factor authentication (MFA) and anti-malware measures to mitigate against capture of the master password by threat actors).

11.1.4 A financial institution should ensure that credentials are unique and not shared among multiple users, processes, services, or systems, and granted in accordance with the needs of the required access.

11.1.5 Where passwords are used, they should be of sufficient complexity and length to protect against common brute-force attacks. A financial institution should also ensure that passwords are regularly changed without reuse and default passwords are changed upon first login. Passwords should be stored securely (e.g., hashed, encrypted, etc.) and not stored in plaintext.

11.1.6 Where password-less solutions are used (e.g., ephemeral certificates, magic links[31], one-time codes, etc.), access to the issuing authority should be stringently controlled with MFA and anti-malware measures to mitigate against capture of the master password by threat actors. The financial institutions should ensure that systems connecting to the issuing authority are appropriately configured to support such access at the point of implementation.

11.1.7 Any third parties, contract or part-time staff, and external systems connecting to corporate resources should adhere to the established credential management process and be subject to the same access restrictions and monitoring as employees of the financial institution.

11.1.8 A financial institution should perform regular reviews of all credentials to verify that they are appropriately managed, with greater frequency of reviews for credentials that have access rights to privileged activities. Measures should be in place to identify and rectify exceptions noted during the review (e.g., dormant, redundant, or wrongfully provisioned credentials) in a timely manner. Where a pattern of exceptions or deviations are noted from reviews, the financial institution should investigate the root cause of the pattern and take appropriate steps to prevent recurrence.

11.1.9 A financial institution that integrates access to its systems with third party credential management solutions (e.g., online credential provisioning services, etc.) or adopts federated identity management solutions to enable access to heterogenous architecture (e.g., SPIFFE and SPIRE)[32], multiple web domains or multiple web services[33], should conduct adequate due diligence on the solution prior to integration. Security characteristics of the solution(s) should be assessed to ensure that the generation and transmission of credentials is secured against threat actors and only requisite data is transmitted.

[31] Magic links are a type of password-less login that allow users to log into an account by clicking a link that's emailed to them, rather than typing in their username and password.

[32] SPIFFE, the Secure Production Identity Framework For Everyone (SPIFFE) Project defines a framework and set of standards for identifying and securing communications between application services. SPIRE (the SPIFFE Runtime Environment) is a toolchain of APIs for establishing trust between software systems across a wide variety of hosting platforms.

[33] Examples of technologies that facilitate federated identity management across web services include Security Assertion Markup Language (SAML), Open Authorisation (OAuth), and OpenID.

11.1.10 A financial institution should ensure that credentials used for privileged activities (e.g., system administration, sensitive computer operations, etc.) have strict approval mechanisms and are granted to competent and trusted users. Such privileged credentials should not be used for activities that do not require privileged access.

11.1.11 All activities performed should be logged with the associated credential tagged for audit and review. Such logs should be inaccessible by the credential generating it and should be reviewed by an appropriate party for any unauthorised or malicious activity on a regular and timely basis.

Desired Outcome 11.2 – Authorisation

11.2.1 In order for credentials to access an asset, they require some form of authorisation by the asset. Such authorisation specifies what type of access rights the credential has and if the credential is able to access the asset at all. Such authorisations are typically defined as policies and multiple credentials can be assigned to such policies. This facilitates assigning access rights to large groups in a controlled and extensible manner.

11.2.2 There are multiple models for authorisation. Access can be granted based on attributes, roles, entities, location, rules, etc. Access can be prescriptive via mandatory access where end users have no ability to change permissions, or discretionary where end users can manage permissions for resources within their authority. Access can also be time-delimited through session-based timeouts to limit persistent access that could be exploited by threat actors targeting idle credentials.

11.2.3 As part of its identity and access management framework, a financial institution should define its authorisation model, the scope of users, processes, services, and systems that should adhere to the framework, and the administrative procedures for creating, modifying, enforcing, deprecating, and deleting policies.

11.2.4 A financial institution should adopt solutions that align with the established authorisation model and authorisation policies should be defined based on the least amount of access necessary for the user, process, services, or system to perform its function i.e., 'least-access principle'. Authorisation policies should also support segregation of duties across the financial institution's functions. The 'never alone principle' should be applied to all access policies associated with privileged activities to ensure that no single user has unilateral access to perform such activities.

11.2.5 Where a certificate authority or equivalent solution is deployed to manage authorisation, a financial institution should ensure that it is configured in accordance with the established authorisation model and all processes or systems relying on it are appropriately configured to recognise the certificates generated for the specified duration.

11.2.6 In line with the principle of least privilege[34], a financial institution should ensure that no person is given unfettered access to data or the corporate network. This includes any individual from senior management or the Governing Body.

11.2.7 A financial institution should perform regular reviews on the access policies and their associated credentials. Measures should be in place to identify and rectify exceptions noted during the review (e.g., expired, redundant, excessive authority, wrongfully assigned credentials, etc.) in a timely manner. Where a pattern of exceptions or deviations are noted from reviews, the financial institution should investigate the root cause of the pattern and take appropriate steps to prevent recurrence.

Desired Outcome 11.3 – Authentication

11.3.1 As technology developed, passwords as a single factor of authentication alone have become insufficient to securely authenticate users, processes, and systems to corporate resources. Threat actors have at their disposable a prolific array of tools to circumvent weak controls to gain unauthorised access to corporate resources. The variety of mechanisms and factors available for authentication today has facilitated greater confidence in drawing information from a myriad of datasets to provide an enriching experience for users.

11.3.2 To enable MFA, credentials are presented with additional factors that typically fall into the following categories.

11.3.2.a Knowledge – Something you know (e.g., password, PIN, etc.)

11.3.2.b Possession – Something you have (e.g., smartcards, tickets, token, OTP, etc.)

11.3.2.c Inherence – Something you are (e.g., biometrics, behaviour, etc.)

11.3.3 As part of its identity and access management framework, a financial institution should define the type(s) of authentication mechanism(s) and factor(s) required to authenticate users, processes, services, and systems based on the criticality of the resource. In particular, MFA should be applied on a risk-based approach, for instance users who access corporate resources remotely, perform privileged activities, or with access to sensitive or critical systems or datasets. Where appropriate, MFA should be required for sensitive customer, business, or operational functions.

11.3.4 A financial institution should ensure that there is a limit to the number of acceptable failed authentication attempts to mitigate against brute force attacks and MFA bypass attacks.

11.3.5 Concurrent access by a single credential should only be enabled based on credible business needs and each access channel authenticated independently.

[34] A credential should only be given the minimum level of access or permissions needed to perform the job functions.

11.3.6 A financial institution that relies on authentication solutions external to the corporate network, should conduct adequate due diligence on the solution prior to integration. Security characteristics of the solution(s) should be assessed to ensure that the generation and transmission of authentication data is secured against threat actors and only requisite data is transmitted.

11.3.7 A financial institution should perform regular reviews on the suitability of the chosen authentication mechanism and associated factor(s). Measures should be in place to identify and rectify exceptions noted during the review in a timely manner. Where a pattern of exceptions or deviations are noted from reviews, the financial institution should investigate the root cause of the pattern and take appropriate steps to prevent recurrence.

One-Time Password (OTP)

11.3.8 OTPs comprising numbers or an alphanumeric set of characters have been delivered on a variety of channels including hardware and software tokens, short message service (SMS), or email.

11.3.9 A financial institution that employs software within a mobile application to generate the OTP or utilises push notifications to send automated generated codes as OTPs should ensure that the OTP generators and authenticators are robust in security design and features to mitigate against hacking attempts from threat actors[35].

11.3.10 Where a third-party software OTP solution is used, a financial institution should conduct adequate due diligence on the solution prior to integration. Security characteristics of the solution(s) should be assessed to ensure that the generation and transmission of the OTP is secured against threat actors and only requisite data is transmitted.

11.3.11 Where SMS is used as the channel to deliver OTPs, a financial institution should have a process in place at the point of onboarding to verify that the phone number registered to receive the SMS indeed belongs to the intended user requiring authentication and not to virtual phone numbers (e.g., VoIP[36]). The financial institution should also ensure that the change process to update registered phone numbers requires MFA to mitigate against SIM-swapping attacks[37].

Biometric Authentication

11.3.12 Biometric authentication solutions may use biological, physiological, or behavioural aspects of an individual to facilitate identification. In developing such authentication

[35] For example, where the software token solution is on a mobile device, mobile application security measures such as detecting and blocking rooted or jailbroken devices should be implemented.
[36] Voice over Internet Protocol (VoIP) enables users to make calls over an internet connection instead of traditional phone lines. Aside from the inherent threat of being hacked by threat actors due to the internet-based nature of the service, threat actors are also known to use VoIP numbers as part of SIM-hijacking attacks.
[37] SIM-swapping attacks occur when a threat actor gains control of a phone number by assuming the victim's identity and persuading their mobile service provider to port the number to a SIM card that is in their possession.

solutions, large datasets are required to train the authentication model to achieve high matching success rates prior to commercial deployment.

11.3.13 In selecting a biometric authentication solution, a financial institution should perform adequate due diligence on key performance metrics[38] and anti-spoofing measures[39] to gain assurance that the solution would perform to expectation, including where appropriate an independent assessment by a suitably qualified professional. Where the solution is deployed to authenticate access to sensitive functions, systems or data, the financial institution should require more stringent key performance metrics. Upon deployment, the financial institution should monitor key metrics of the biometric authentication solution to evaluate performance and undertake remedial actions when the metrics fall below acceptable benchmarks.

11.3.14 Regardless of the deployment model[40] of the biometric authentication solution, a financial institution should ensure that robust security controls are in place measures to mitigate against compromise or unauthorised access of biometric data or templates by threat actors. Biometric data and templates should be encrypted in storage and in transmission and a process established for the revocation and replacement of compromised biometric data or templates.

11.3.15 A financial institution should establish procedures that verify the user enrolling to the biometric authentication solution (e.g., in-person enrolment, cross referencing government-issued identity document, etc.). The enrolment process should be administrated by qualified personnel or staff who have been adequately trained to conduct enrolment correctly.

11.3.16 A financial institution should adhere to any regulatory obligations applicable to the protection of biometric data and templates.

Single Sign On (SSO)

11.3.17 While SSO facilitates productivity and reduces friction in user experience, it can be a significant source of risk if not adequately secured against threat actors that exploit SSO to gain unfettered unauthorised access to systems and data.

11.3.18 A financial institution that enables SSO should ensure that the SSO policy server or equivalent is configured and kept up to date with the financial institution's established authorisation policies. It should log SSO tokens activities for audit and review. Where SSO is employed for access to sensitive systems and data, the financial institution should apply MFA.

11.3.19 Where a third-party SSO solution is used, a financial institution should conduct adequate due diligence on the solution prior to integration. It should assess the security

[38] These metrics include false acceptance rates and false rejection rates.
[39] For example, voice matching with enrolled voiceprint, face matching with identity document, liveness detection during video capture, blood flow detection during fingerprint scanning, etc.
[40] Biometric data and templates may be stored centrally on a server managed by the financial institution or a third-party, or stored in a distributed manner on user mobile devices.

characteristics of the solution(s) to ensure that the generation and transmission of the SSO token is secured against threat actors and only requisite data is transmitted.

Chapter 12 – Online Transaction Security

Desired Outcomes for Online Transaction Security

Desired Outcome 12.1 – Online Transaction Security: A financial institution should design its systems and processes with the aim of reducing the potential for fraudulent activity taking place via its online financial services.

Desired Outcome 12.2 – Fraud Mitigation: A financial institution should implement capabilities to detect and mitigate fraudulent activities on its online financial services.

Desired Outcome 12.3 – Customer IT Risk Awareness: A financial institution should regularly inform customers of the risks associated with the use of online financial services.

12.0.1 The provision of financial services online brings significant benefits to both financial institutions and customers. However, as financial institutions move from only provisioning informational services online to including transactional services in the online platforms, the risk of threat actors exploiting such advancements is high. Financial institutions should secure their online transactional services to prevent risk events from materialising and causing significant disruption to their business operations and distress to customers.

Desired Outcome 12.1 – Online Transaction Security

12.1.1 A financial institution that enables customers to access financial services through its online platforms should implement MFA at login.

12.1.2 A financial institution should implement authentication mechanisms for high-risk activities (e.g., adding payee, updating contact information and limits, etc.) performed by customers through online financial service platforms. Such authentication mechanisms could include transaction signing with digital certificates, behavioural analysis, etc.

12.1.3 Where MFA is applied for high-risk transactions, the MFA request should be distinct, and where practical, a different channel from the MFA request used for login. Such an implementation increases the difficulty that a threat actor would need to overcome to compromise a customer's account.

12.1.4 A financial institution should ensure that upon login to the online financial service platform by a customer, each authenticated session is time-delimited, measures are implemented to prevent session hijacking, and the session is terminated promptly when a compromise is detected.

12.1.5 A financial institution should disallow network protocols that are used with the intention of obfuscating identity or attribution[41] from performing login or high-risk transactions on its online financial services to reduce the likelihood of threat actors exploiting financial services for criminal gains.

12.1.6 Prior to exposing any financial services on third-party mobile communications platform (e.g., voice or messaging mobile application) or via third-party providers (e.g., payment intermediaries), a financial institution should conduct adequate due diligence on the platform prior to integration. Security characteristics of the platform or services should be assessed to ensure that it is secured against threat actors and only requisite data is transmitted. The financial institutions should also perform a risk assessment to determine the scope of financial services that would be suitable for its interaction with customers over such platforms or services.

12.1.7 Where a financial institution utilises third-party mobile communications platform and/or social media platforms to provide financial services, appropriate controls should be in place to adequately authenticate customers prior to onboarding via the platform. Where high-risk transactions are made available via such platforms, a financial institution should implement MFA consistent with the MFA applied to high-risk transactions performed on the financial institution's online transactional platform.

12.1.8 Where financial services are facilitated through third-party providers, financial institutions should ensure that the onboarding of customers to the third-party provider is aligned with the authentication process for login to the financial institution's online transactional platforms. The financial institution should ensure that its integrations with the third-party provider include monitoring controls to detect and mitigate fraudulent transactions.

Desired Outcome 12.2 – Fraud Mitigation

12.2.1 While financial institutions implement various security controls to authenticate customers and secure online transactional services, fraudulent transactions still occur as threat actors innovate and develop techniques to work around security controls. For example, social engineering attacks on customers enable threat actors to obtain the necessary information to legitimately access customers' accounts and conduct fraudulent transactions.

12.2.2 A financial institution should implement systems or mechanisms to detect suspected fraudulent activities on its online transactional services. Such systems or mechanisms include detection of suspicious login activities, real-time fraud surveillance capabilities, transaction pattern deviation analysis, abnormal system activities, etc. The financial institution should notify customers of detected suspected fraudulent activities in a timely manner.

[41] Examples of such protocols include The Onion Router (Tor) and the Invisible Internet Project (I2P). These protocols encrypt and transmit communications through a network of servers resulting in the end-recipient being unable to determine the true origin of the communication.

12.2.3 A financial institution should establish processes and procedures to provide customers a means to promptly inform the financial institution of potentially fraudulent activity and to replace compromised credentials.

12.2.4 A financial institution should establish processes and procedures to investigate potentially fraudulent activities that have been detected through its surveillance or reported by customers. Such processes and procedures should include classification of suspected fraudulent activities by severity, technical activities for issue resolution, escalation protocols and reporting, and integration into the financial institution's incident management framework and business continuity plan where appropriate. The financial institutions should also engage the affected customer(s) to ensure they are apprised of the investigation progress and outcome in a timely manner.

Desired Outcome 12.3 – Customer IT Risk Awareness

12.3.1 Akin to how financial institutions are expected to inform customers of associated risks prior to subscribing to financial products, financial institutions should inform customers of the respective rights, obligations and responsibilities of the customers and the financial institution on all matters relating to online transactions, and of the associated risks with the use of the financial institutions' online financial services.

12.3.2 Such information should be provided prior to customers' use of the financial institution's financial services and then regularly as the customer continues to interact via the online transactional service. The information provided to customers should include prevalent techniques used by threat actors to target customers and mitigating actions that customers can take to avoid becoming a victim of compromise.

12.3.3 When a financial institution updates its online financial service platforms with new interfaces or functionalities, the financial institution should provide its customers with adequate instruction or information to familiarise customers with the updates.

Desired Outcomes for Cryptography

Desired Outcome 13.1 – Cryptographic Schemes: A financial institution should implement secure cryptographic schemes.

Desired Outcome 13.2 – Key Lifecycle Management: A financial institution should ensure cryptographic keys are managed securely throughout its lifecycle.

13.0.1 All cryptographic schemes comprise an algorithm and a key with the latter being the secret. The purpose of adopting cryptographic schemes is to protect the integrity and confidentiality of information that a financial institution determines as sensitive. Use of cryptographic schemes extends beyond data encryption at rest or transit and signature or certificate verification to API authentication and immutable recording of information.

Desired Outcome 13.1 – Cryptographic Schemes

13.1.1 A variety of cryptographic schemes are used across a financial institution's IT implementation. A financial institution should therefore ensure that the appropriate cryptographic scheme is applied to best suit the security requirements of each use case. Where possible, well-established internationally recognised and tested cryptographic schemes should be adopted, configured to the most up-to-date security standards (e.g., key size, hash function, random function, etc.), and deployed in a manner optimised for the financial institution's implementation. All deployment of cryptographic schemes should be in accordance with the financial institution's established system development and testing framework.

13.1.2 As technology advances, new techniques to overcome cryptography become available. Financial institutions should maintain an awareness of industry developments to ensure that their adopted cryptographic schemes remain resistant to such new techniques and update their outdated schemes with contemporary ones that are able to provide the required protection.

13.1.3 Where a financial institution manages its own public key infrastructure for the management of digital certificates, the financial institution should ensure that the supporting functions (e.g., certificate authority, registration authority, central directory, certificate policy and the certificate management system, etc.) are securely configured, and controls implemented to protect them from compromise.

13.1.4 Where a third-party public key infrastructure solution is used, a financial institution should conduct adequate due diligence on the third party prior to integration. Security characteristics of the solution should be assessed to ensure public key infrastructure is secured against threat actors.

13.1.5 Financial institutions should evaluate the need for implementing post-quantum cryptography (PQC) or quantum key distribution (QKD) capabilities for sensitive

datasets and network communications. For example, in relation to the threat of 'harvest now, decrypt later'[42], financial institutions should assess the need to protect high-value data and communications that need to remain encrypted for the long term.

Desired Outcome 13.2 – Key Lifecycle Management

13.2.1 The secure management of cryptographic keys is essential to the effective use of cryptographic schemes. Where a financial institution administers its own cryptographic keys, policies and procedures on the secure generation, distribution, use, storage, renewal, revocation, recovery, and destruction should be established.

13.2.2 A financial institution should ensure that keys are generated securely from cryptographic modules (hardware or software) using strong encryption algorithms. The generated keys should be stored in secure facilities such as physical or virtual hardware security modules, vaults, securely managed by a secrets management service, etc. Keys should not be hard coded into source code and should not be stored in the same location as the encrypted data. Backups of the keys should be accorded equally stringent security controls. The cryptographic key generation ceremony should be restricted to only the necessary and competent personnel.

13.2.3 When cryptographic keys are used, transmitted, or transported, financial institutions should ensure that appropriate measures such as encrypting or 'wrapping' the keys are in place to protect against attacks on the keys' integrity or interception by threat actors.

13.2.4 Where the cryptographic scheme requires multiparty computation[43], the financial institution should ensure that each key part is stored securely, and parts distributed to various parties are done so in a secure manner.

13.2.5 A financial institution should ensure that cryptographic keys are used for their specified purpose for the specified duration. The financial institution should ensure that controls are in place to prevent single use keys from being re-used or any keys being used beyond their expiry.

13.2.6 A financial institution should ensure that its systems do not enable keys that have been revoked or expired to be used. A financial institution should implement measures for the timely and secure destruction of revoked or expired keys to prevent them being reused by threat actors.

13.2.7 The financial institution should maintain an up-to-date inventory of all keys either generated or procured from third parties. The inventory should be reviewed and updated regularly.

[42] 'Harvest now, decrypt later' is a practice where threat actors collect and store stolen or leaked datasets in anticipation of quantum computers being capable of decrypting today's encryption methods thereby enabling threat actors to subsequently extort from the organisations to whom the datasets belong.
[43] A cryptographic key is split into Y number of parts for use by multiple parties and an X of Y combination is required for computation.

13.2.8 Where keys are to be replaced or renewed, a financial institution should ensure that the process to replace or renew the key does not allow for threat actors who have unauthorised access to the old key are able to derive the new key. Financial institutions should ensure that keys are rotated to reduce the likelihood of key theft by threat actors.

13.2.9 If a key is compromised (e.g., modified or intercepted by threat actor, secrets leak made public on the internet, vulnerability in cryptographic scheme, etc.), the financial institution should assess if the compromise extends to other keys or the overall cryptographic scheme and take appropriate action to replace the affected keys or scheme and to destroy all compromised keys.

13.2.10 A financial institution that relies on a third-party key management service should ensure that the appropriate security configurations are enabled or provisioned to securely manage keys throughout their lifecycles. Adequate due diligence on the third party should be performed prior to engagement, and ongoing oversight over the performance of the service should be maintained by the financial institution.

13.2.11 A financial institution should ensure that all activities involving keys are logged and monitored. Such logs should be reviewed by an appropriate party for any unauthorised or malicious activity on a regular and timely basis.

SECTION D: LEVERAGING BUSINESS EMBEDDED TECHNOLOGIES

Chapter 14 – Algorithm Driven Solutions

Desired Outcomes for Algorithm Driven Solutions

Desired Outcome 14.1 – Governance of Algorithm Driven Solutions: A financial institution should have appropriate governance structures to support sound development and usage of algorithm driven solutions.

Desired Outcome 14.2 – Safe Development and Usage: The use of algorithm driven solutions should not compromise a financial institution's ability to conduct its business operations or services to customers in accordance with applicable laws and its ethical norms.

Desired Outcome 14.1 – Governance of Algorithm Driven Solutions

14.1.1 The use of machine learning techniques and artificial intelligence systems have enabled greater automation of tasks and spurred new possibilities for building business processes. From the introduction of algorithmic trading to the use of 'robo-advisors' for customised financial portfolio management, and more recent developments of generative artificial intelligence models and quantum computing algorithms, the use of algorithms in varying degrees of complexity have brought positive outcomes for the benefit of customers.

14.1.2 As these techniques and systems advance, the underlying algorithms become more complex and, without adequate governance, may reach a state where the output no longer meets the desired objectives or results in unexpected consequences[44]. Financial institutions that make use of algorithm driven solutions ('ADS') should be cognisant of the associated risks and ensure that business operations and services to customers are not compromised by poor control over the ADS used.

14.1.3 A financial institution should establish a governing framework to ensure that all ADS used adhere to clearly defined principles, fall within the established risk management framework and risk appetite for model behaviour, and system development policies. The framework should be reviewed regularly and approved by the financial institution's senior management and Governing Body. The framework should encapsulate policies and procedures for the development, use, monitoring, maintenance, and cessation of ADS, both internally developed or sourced externally.

14.1.4 The framework should include a materiality classification applicable to ADS assessing for the model's complexity and impact of an outcome (e.g., customer impact, regulatory breach impact, financial impact, etc.). ADS that are more material should be held to

[44] For example, artificial intelligence models may 'hallucinate' i.e., generate false or misleading results based on perceived patterns.

higher standards of model design and more stringent controls to prevent model compromise.

14.1.5 The design of the governance framework, the development or acquisition of ADS, and the ongoing management of ADS should be performed by competent staff who have the requisite expertise. Where ADS are involved in supporting business functions, the relevant staff with the business expertise should be involved to ensure the ADS is aligned to achieving the required business objectives.

14.1.6 The governance framework should include assigning accountability for each ADS to an appropriate and responsible senior executive to ensure that the ADS is managed in line with the governance framework.

14.1.7 For each ADS, the financial institution should establish the desired objectives and expected outcomes. The financial institution should have processes and/or tools in place to detect and remediate erroneous or undesirable outcomes generated by the ADS.

14.1.8 A financial institution should ensure that all ADS developed internally adhere to established secure system development practices, are approved by the appropriate level of management, and robust functional and non-functional testing is performed prior to use[45]. The financial institution should ensure that the ADS model is trained on the appropriate quality and quantity of data to accurately achieve the desired objectives consistently. The financial institution should ensure that any updates to the ADS model are conducted in line with the established system development and testing framework and that the updated ADS model is tested to ensure that it is aligned with the established ADS governance framework.

14.1.9 ADS sourced externally should minimally meet the financial institution's established governance framework's requirements. The financial institution should perform adequate due diligence to fully understand the sourced ADS model design to ensure that desired objectives are achieved as advertised. Any updates provided by the sourced ADS' vendor should be similarly reviewed and tested prior to acceptance and deployment.

14.1.10 Where a financial institution enables its employees to utilise ADS in a manner akin to EUC (e.g., use of publicly accessible ADS online), the financial institution should incorporate into its ADS governance framework acceptable use policies that outline the expectations surrounding the use of ADS in EUC. Such policies should set out the scenarios where use of ADS in EUC is acceptable, scenarios where ADS in EUC should not be used, the handling of data when interacting with ADS, and reporting mechanisms for violations to the policies.

[45] For example, financial institutions can refer to the OWASP top 10 for Large Language Model Applications.

Desired Outcome 14.2 – Safe Development and Usage

14.2.1 Where a financial institution develops ADS to serve as a tool for business decisions, the established governing framework should incorporate the following:

14.2.1.a The financial institution should be able to provide clear explanations on what data was used by the ADS and the decision process that led to an output[46].

14.2.1.b ADS should be designed to maintain decision parameters that are aligned with the financial institution's ethical norms.

14.2.1.c ADS do not systematically disadvantage any individual or groups of individuals unless justified, and comply with all applicable laws.

14.2.2 Where a financial institution intends to incorporate a 'human-in-the-loop' design consideration into an ADS to improve outcomes and mitigate biases, the financial institution should ensure that the appropriate and responsible staff is/are adequately trained in the ADS and for the role(s) to be performed, and escalation procedures are in place to manage issues arising from the use of the ADS.

14.2.3 Where a financial institution exposes an ADS for interaction with external parties (e.g., customers), the financial institution should ensure that the ADS is regularly reviewed for compromise resulting from attacks by threat actors. Such attacks include model or data poisoning[47], model or data extraction[48], denial-of-service[49], etc.

14.2.4 Where the ADS makes use of data from external parties (e.g., customers) for decision making that impacts those external parties, the external parties should be informed that they are interacting with an ADS, given adequate information on interacting with the ADS[50], and the associated risks and limitations of the ADS.

14.2.5 A financial institution should regularly test and validate its developed ADS models for accuracy, performance, errors, or unintentional biases both in the decision points and in the data supplied to the model. Where practical, such tests should also measure the ADS' adherence to the established governance framework.

14.2.6 Where over time the ADS model has drifted beyond the parameters defined in the ADS governance framework, the financial institution should review the suitability of the ADS

[46] For example, financial institutions can leverage on interpretability or transparency techniques such as coefficients of logistic regressions, LIME, Shapley values techniques (QII, SHAP), and integrated gradient explanations.
[47] Such attacks arise when a threat actor attempts to provide large volumes of malicious input that would skew the ADS decision making towards the intended malicious outcome.
[48] Model or data extraction attacks are performed to extract information about an ADS such as its architecture or decision parameters.
[49] A denial-of-service attack on an ADS involves attempts to disrupt the performance by flooding the ADS with queries that would exhaust the computation resources of the ADS.
[50] For avoidance of doubt, such information does not include exposure of the financial institution's intellectual property, proprietary source code or details on sensitive or confidential internal processes.

solution and take appropriate steps to either recalibrate the model where possible or cease its use.

14.2.7 A financial institution should ensure that the use of ADS does not weaken existing controls. For example, prior to granting an ADS solution access to sensitive or critical data, adequate safeguards should be in place to ensure that the users of the ADS also have the requisite access rights to interact with such data.

Desired Outcomes for Decentralised Infrastructure Solutions

Desired Outcome 15.1 – Understanding Decentralised Infrastructure Solutions: A financial institution should establish a clear understanding of the nature and nuances of each decentralised infrastructure solution it interacts with.

Desired Outcome 15.2 – Secure Participation: A financial institution should ensure that its resources interacting with the decentralised infrastructure solution are securely managed.

Desired Outcome 15.1 – Understanding Decentralised Infrastructure Solutions

15.1.1 The rise of distributed ledger technology has the potential to transform financial services and is increasingly being adopted by financial institutions. Distributed ledger technology can be combined with other technologies to create decentralised infrastructure solutions where activities take place both on and off the blockchain. As these technologies develop and grow in complexity, potential unique risks arise that require financial institutions to develop specific expertise to manage those risks.

15.1.2 This Guidance will focus on the associated IT risks arising from the adoption of decentralised infrastructure solutions ('DIS'). To provide guiding principles around which financial institutions can build their risk management frameworks, the following can be considered as key features that would be associated with decentralised infrastructure solutions.

15.1.2.a Multiple participants[51] in the network can be individually **responsible** for the execution of a task;

15.1.2.b Multiple participants in the network can be individually **accountable** for validating the successful execution of a task;

15.1.2.c The successful execution of a task is broadcast to the network to keep participants **informed** for the purpose of maintaining a collectively accepted record of successfully executed tasks; and

15.1.2.d Multiple participants can be **consulted** on and individually vote on changes to be made to the operation of the network and the scope of tasks permissible for future execution by participants.

15.1.3 These features may manifest in varying forms depending on the intended objectives and development maturity of the DIS. These features distinguish decentralised systems from distributed systems. Distributed systems typically still have a central point of responsibility or shared responsibility across designated participants to execute tasks.

[51] An underlying assumption is that participants in the network can be external to and not controlled by a financial institution.

15.1.4 Financial institutions adopting solutions that purport decentralisation or intending to participate in DIS should be cognisant of the specific IT risks arising from the nature of such solutions.

Desired Outcome 15.2 – Secure Participation

15.2.1 A financial institution should establish a governing framework to ensure that all DIS participation adhere to clearly defined principles and system development policies. The framework should be reviewed regularly and approved by the financial institution's senior management and Governing Body. The framework should encapsulate policies and procedures for the participation and monitoring of DIS, both internally developed or connected to externally.

15.2.2 A financial institution should ensure that prior to connecting to or integrating its assets to a DIS and its participants, adequate due diligence on the governance (e.g., consensus mechanism, finality, fees, forking policies, ownership of governance tokens, control of smart contracts, etc.), technical specifications (e.g., cryptographic scheme, hardware and software requirements, network architecture, etc.), components (e.g., tokens, nodes, oracles[52], cross-chain interoperability[53], etc.), and track record of the DIS is performed. A financial institution should also ensure that it maintains ongoing oversight of the DIS throughout its participation.

15.2.3 Where a financial institution develops its own DIS, it should ensure appropriate safeguards are in place to prevent facilitating potential criminal activities on the DIS (e.g., anonymous participation should not be allowed, etc.).

15.2.4 A financial institution that performs activities on DIS should utilise appropriate tools to monitor the status of the network and trace relevant published activities that pertain to the financial institution's activities in the DIS.

15.2.5 A financial institution should ensure that any data it submits and writes into the DIS does not result in breaches to any regulatory obligations (e.g., personal data, illegal material, etc.). If sensitive data is necessary to interact with the DIS, appropriate measures should be taken to protect sensitive data (e.g., encrypted, hashed, etc.).

15.2.6 A financial institution that participates in a DIS that facilitates the transfer of digital assets should employ tools that trace transactions and gather associated transaction information (e.g., originator, receiver, sanctions, etc.) for review against requisite anti-money laundering and targeted financial sanctions, laws, regulations, guidance, and notices. The financial institution should have processes in place to address any findings in accordance with the requirements.

15.2.7 Where a financial institution operates a component to contribute to a DIS that is not core to its business operations and services to customers, the financial institution

[52] Oracles are components in a blockchain network that facilitate the provision of off-chain data into the blockchain network enabling smart contracts to execute transactions based on the provided data e.g., real-time forex data, etc.
[53] Cross-chain interoperability refers to integrations or protocols that facilitate the communication of data between separate blockchains that may have disparate data formats and requirements.

should ensure that the resources required to operate the component (e.g., storage, memory, operating system, cryptographic keys, etc.) are separate from resources required to operate its IT environment that supports its business operations and services to customers. The financial institution should ensure that the operated component is configured to the requisite security configuration and any technical updates are applied in a timely manner.

15.2.8 Where a financial institution is expected to exercise its obligation to elect on changes on the DIS, relevant competent personnel from the financial institution should be involved in making a decision. The financial institution may establish an internal function or forum to coordinate such decision making with the appropriate level of management approval.

15.2.9 A financial institution should monitor the DIS to ensure that when participation is no longer tenable for technical (e.g., known compromises to the protocol, compromises to oracle source data, performance degradation, etc.), legal, or regulatory, (e.g., abusive material published on immutable blockchain platform, etc.) reasons, steps are taken to extract or liquidate any remaining assets from the DIS in a safe and timely manner. All IT resources used to support the financial institution's activities on the DIS should be securely disconnected from the DIS network.

15.2.10 As DIS operate on the premise that there is no SPOF, a financial institution should ensure that its business continuity policies and procedures pertaining to its IT resources participating in the DIS are established with the recognition that failure of individual components in the DIS may not result in complete loss of data or effect a disruption to the entire DIS network.

15.2.11 A financial institution should incorporate the monitoring of its participation (e.g., components operated by the financial institution, etc.) in the DIS into its cyber event monitoring solutions or services.

Programmable Contract Security

15.2.12 A financial institution that publishes programmable contracts for transaction automation on a DIS should ensure that secure system development practices are adhered to, and robust testing is performed prior to publication.

15.2.13 Prior to transacting with programmable contracts created by third parties, a financial institution should perform adequate due diligence to assess code integrity, code security, and code alignment to the intended transacting outcome(s) of the programmable contract, including any other programmable contract(s) called upon to execute a transaction. A financial institution should re-perform such due diligence following updates to the programmable contract.

Digital Wallet Security

15.2.14 Where a financial institution administers its own digital wallets (e.g., hot, cold, warm, etc.) for custody of digital assets, the financial institution should ensure that the

generation, access, use, revocation, recovery, and destruction of its keys and wallets adhere to established policies and procedures. The keys associated with each wallet should be securely managed in accordance with the financial institutions policies and procedures for key lifecycle management.

15.2.15 Financial institutions should ensure that seed phrases[54] are stored securely with adequate backup copies of the seed phrases in secure locations.

15.2.16 Where a financial institution engages a third party for digital wallet services, adequate due diligence on the third party should be performed prior to engagement, and ongoing oversight over the performance of the service should be maintained by the financial institution. The financial institution should have clarity on its responsibilities in managing the digital assets and the extent of control it holds with regard to initiating transactions prior to entering into such arrangements.

15.2.17 Financial institutions should ensure that adequate controls are in place to detect and mitigate against wallet attacks that exploit automation, e.g., velocity limits, multi-factor authentication for transfers between wallets, etc.

15.2.18 A financial institution that maintains cold wallets should ensure that they are stored on secure hardware devices assigned to appropriate personnel, regularly backed up, and are accounted for as part of the financial institution's asset inventory.

[54] Seed phrases are a sequence of words that service as a backup to the wallet's private key. Seed phrases can be used to regain access to digital assets in the event the original wallet is unavailable.

ANNEX A: RELATED ADGM RULES, REGULATIONS AND GUIDANCE

A financial institution in the ADGM should be cognisant of applicable rules and guidance. The table below illustrates the landscape of rules and guidance that include IT-related content. These rules and guidance issued by the Relevant ADGM authorities are available at https://en.adgm.thomsonreuters.com/.

Regulations and Rulebooks containing IT-related content	**ADGM Regulations**	• Data Protection Regulations 2021 • Electronic Transactions Regulations 2021	
	FSRA Rules (Activity-agnostic)	• General Rulebook (GEN) • Anti-Money Laundering and Sanctions Rules and Guidance (AML)	
	FSRA Rules (Activity-focused)	• Conduct of Business Rulebook (COBS) • Prudential – Investment, Insurance Intermediation and Banking Rules (PRU) • Prudential – Insurance Business (PIN) • Market Infrastructure Rulebook (MIR)	
Guidance containing IT-related content	**FSRA Guidance (Thematic)**	**Activity/Topical-Focused** • Digital Securities • Digital Investment Management ("Robo-advisory") • Private Financing Platforms and Multilateral Trading Facilities dealing with Private Capital Markets • Virtual Assets • Governance Principles and Practices to Mitigate Cyber Threats and Crime	**Technology-Focused (Activity-agnostic)** • Application Programming Interfaces (APIs) • Enabling Technologies (Joint-issuance with CBUAE, SCA, and DFSA)
	FSRA Guidance (Activity-agnostic)	Information Technology Risk Management Guidance	