INFORMATION TECHNOLOGY POLICY

Standard Capital Markets Limited

Standard Capital Markets Limited
[Company address]

Table of Contents

1. Policy Statement 1
2. Definitions & Interpretations 2
3. Objective of the Policy 4
4. Applicability & Scope of the Policy 5
5. Key Focus Areas of IT Governance 6
6. Governance Structure of IT Framework 7
7. Roles & Responsibilities within Governance Structure 10
8. IT Service Management Framework 16
9. Outsourcing Arrangements 17
10. Capacity Management of IT Resources 18
11. IT Project Management Framework 19
12. Change & Patch Management 21
13. Data Migration/Transfer Mechanism 22
14. Audit Trails & System Logging 23
15. Cryptographic Standards 23
16. Physical & Environmental Security Controls 24
17. IT Access Control Measures 24
18. IT Performance and Metrics 25
19. Information Security Management Framework 26
20. Cyber Security Management Framework 27
21. Risk Assessment Framework 27
22. Vulnerability Assessment (VA)/Penetration Testing (PT) 28
23. Business Continuity and Disaster Recovery Management 29
24. Information System (IS) Audit 30
25. Approval, Review & Update 31

DOCUMENT IDENTIFICATION INFORMATION

Document Name	Information Technology Policy
Index	Corporate Governance/ IT Governance/ Compliance/ Information Technology Policies & Strategies
No. of Pages	33
Approving Authority	Board of Directors
Review Frequency	At least once a year or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

This policy is issued by Standard Capital Markets Limited (hereinafter referred to as "SCML" or "Company").

1. Policy Statement

1.1. The Information Technology Policy (he*reinafter referred to as "IT Policy"*) of SCML is established to ensure robust governance, management, and control of Information Technology systems and infrastructure. The policy aims to align SCML's IT strategy with its business objectives while mitigating risks associated with IT operations.

1.2. This policy outlines the framework for managing IT risks, implementing controls, and ensuring compliance with regulatory requirements, thereby safeguarding the confidentiality, integrity, and availability of information assets. The Policy also defines the roles and responsibilities of the Board, management, and employees in maintaining IT security and resilience.

1.3. This policy is formulated in compliance with Clause 5(a) of the *Reserve Bank of India's (RBI) Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices, issued on November 7, 2023,* which mandates the adoption of IT governance and risk management practices to ensure business continuity and resilience in the face of evolving technology risks.

2. Definitions & Interpretations

2.1. In this IT Policy, unless the context specifies otherwise, the following terms shall have the meanings ascribed to them below:

2.1.1. Cyber: Refers to anything relating to, within, or through the medium of the interconnected information infrastructure, encompassing interactions among individuals, processes, data, and information systems.

2.1.2. Cyber Event: Any observable occurrence within an information system. Cyber events can serve as indicators that a cyber incident may be happening.

2.1.3. Cyber Security: The practice of preserving the confidentiality, integrity, and availability of information and/or information systems through the cyber medium. It also encompasses other related properties such as authenticity, accountability, non-repudiation, and reliability.

2.1.4. Cyber Incident: A cyber event that negatively impacts the cyber security of an information asset, whether resulting from malicious activity or accidental causes. The term 'incident' implies 'cyber incident' in this Policy.

2.1.5. Cyber-Attack: A deliberate and malicious attempt to exploit vulnerabilities via the cyber medium, intending

to harm, disrupt, or gain unauthorized access to information assets.

2.1.6. De-militarized Zone (DMZ): A network segment that acts as a buffer, logically positioned between internal and external networks to enhance security.

2.1.7. Information Asset: Any piece of data, device, or component that supports information-related activities. This includes information systems, data, hardware, and software.

2.1.8. Information System: A set of applications, services, IT assets, or other components designed for handling information, which includes the operating environment and network systems.

2.1.9. IT Risk: The business risk associated with the use, ownership, operation, involvement, influence, or adoption of IT within the company.

2.1.10. Privileged User: A user who, by virtue of their function or role, is granted elevated access within an information system, with powers significantly greater than those of standard users.

2.1.11. Substantial IT expertise: It means the person has a minimum of seven years of experience in managing information systems and/or leading/ guiding technology/ cybersecurity initiatives/ projects. Such a member should also understand the business processes at a broader level and the impact of IT on such processes.

2.1.12. Technically competent: It shall mean the ability to understand and evaluate information systems and associated IT/ cyber risks.

2.1.13. Straight Through Processing (STP): It is an automated transaction processing method used primarily in the

financial industry that enables the seamless movement of transactions through various systems without manual intervention. By integrating different applications and systems, STP enhances operational efficiency, accuracy, and speed, allowing for real-time processing of transactions.

2.1.14. Data Centre refers to primary data centre for a given application/system and DR its Disaster Recovery site/alternate site.

2.1.15. Metrics are quantifiable measures used to assess the performance, efficiency, and effectiveness of a system, process, or operation. In the context of IT, metrics help organizations track and evaluate system performance, recovery capabilities, security, and alignment with business goals.

2.1.16. Recovery Point Objective (RPO) is the maximum acceptable amount of data loss measured in time. It defines the point in time to which data must be recovered following a disaster or data loss event. For example, if an RPO is set to 1 hour, the organization must be able to recover all data up to one hour before the event.

2.1.17. Recovery Time Objective (RTO) is the maximum acceptable duration of downtime after an incident. It refers to the time it takes to restore normal operations and recover from a disruption. For example, if an RTO is set to 2 hours, the organization must resume its operations within 2 hours of the disruption.

3. Objective of the Policy

3.1. The objective of this IT Policy is to establish a comprehensive framework for the governance, management, and security of

the information technology (IT) systems and infrastructure within SCML.

3.2. The policy aims to ensure the alignment of IT initiatives with SCML's overall business strategy, promote operational efficiency, mitigate IT-related risks, and protect the confidentiality, integrity, and availability of information assets.

3.3. This policy is formulated to:

3.3.1. Ensure compliance with regulatory requirements, particularly issued by the Reserve Bank of India (RBI) Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices.

3.3.2. Strengthen IT governance and risk management practices to safeguard against evolving cyber threats and vulnerabilities.

3.3.3. Define roles, responsibilities, and accountability for IT management across SCML.

3.3.4. Ensure the effective use of IT resources, including data security, disaster recovery, and business continuity planning.

3.3.5. Foster a secure IT environment that upholds the principles of cybersecurity, data privacy, and IT resilience.

3.4. Through this policy, SCML seeks to provide a structured approach to IT operations, supporting long-term business growth while mitigating risks associated with technology.

4. Applicability & Scope of the Policy

4.1. The IT Policy applies to all employees, departments, business units, subsidiaries, and third-party service providers of SCML, including those who interact with, manage, or have

access to SCML's IT infrastructure, systems, applications, data, and related resources.

4.2. The Policy covers all aspects of IT governance, cybersecurity, data protection, risk management, and IT operations, including the use of hardware, software, networks, and cloud-based services. The policy also governs the protection of information assets and compliance with regulatory requirements.

4.3. This policy is applicable across all geographic locations where SCML shall operate and shall be followed by all employees and stakeholders as a mandatory requirement for maintaining IT governance and security.

5. Key Focus Areas of IT Governance

5.1. SCML is committed to establishing and maintaining a robust IT Governance Framework that aligns with regulatory requirements, particularly the RBI Master Direction.

5.2. The IT Governance Framework of the company focuses on the following core areas:

5.2.1. Ensuring that the IT strategy aligns with the business strategy of SCML to support key business objectives and goals.

5.2.2. Managing both inherent and potential IT-related risks, including cybersecurity risks, through continuous monitoring, assessment, and mitigation.

5.2.3. Optimizing the use of IT resources, including personnel, technology, and capital, to maximize efficiency and achieve value.

5.2.4. Regular monitoring and evaluation of IT operations to ensure optimal performance, cost-effectiveness, and compliance with regulatory standards.

5.2.5. Ensuring the resilience of IT systems by preparing for, responding to, and recovering from IT disruptions, including cyber incidents.

6. Governance Structure of IT Framework

6.1. SCML establishes a governance structure to oversee IT management and operations, incorporating the following key components:

Sr. No.	Governance Body	Composition	Reporting Authority	Meetings Frequency
1.	**Board of Directors**	All Board Members	Reserve Bank of India & Shareholders	Annually
2.	**Board level-IT Strategy Committee (ITSC)**	1.Minimum of three directors as members. 2. The Chairperson of the ITSC shall be an independent director and have substantial IT expertise in managing/ guiding information technology initiatives; and 3. Members are technically competent	Board of Directors	Quarterly
3.	**Senior Management**	1. Chief Financial Officer (CFO) 2. Chief Compliance Officer (CCO)	Board of Directors	Quarterly or as when required

		3. Chief Information Security Officer (CISO) 4. Chief Technology Officer (CTO) 4. Head of Human Resources (HR)		
4.	**IT Steering Committee**	Includes Representation at Senior Management level from IT and Business Functions.	ITSC, MD	Quarterly
5.	**Risk Management Committee of the Board (RMCB)**	Board Members, Senior Management	Board of Directors	At least yearly
6.	**Information Security Committee (ISC)**	1.Chief Information Security Officer (CISO) and other representatives from business and IT functions, etc., as decided by ITSC. 2. The head of the ISC shall be from risk management vertical.	ITSC, MD	Regularly, as required
7.	**Head of IT Function (CTO/CIO)**	Senior level, technically competent and experienced official in IT related aspects	ITSC, MD	N/A Ongoing oversight
8.	**Chief Information**	A senior level executive (preferably in the rank of	1.The CISO shall directly	N/A

	Security Officer (CISO)	a General Manager or an equivalent position) The company shall ensure that: 1.The CISO has the requisite technical background and expertise. 2.She/He is appointed for a reasonable minimum term. 3. The CISO's Office is adequately staffed with people having necessary technical expertise, commensurate with the business volume, extent of technology adoption and complexity; and 4. The budget for the information/ cyber security is determined keeping in view the current/ emerging threat landscape.	report to the Executive Director or equivalent executive overseeing the risk management function. 2. The CISO shall not have any direct reporting relationship with the Head of IT Function and shall not be given any business targets.	
9.	**Audit Committee of the Board**	The Audit Committee is required to be constituted of a minimum of three directors as its members as per sub- section 177(2)	Board of Directors	At least annually

of the Companies Act 2013.

7. Roles & Responsibilities within Governance Structure

7.1. Board of Directors

7.1.1. The Board approves all strategies and policies related to Information Technology (IT), Information Assets, Business Continuity, Information Security and Cyber Security (including Incident Response and Recovery Management/Cyber Crisis Management).

7.1.2. The Board conducts an annual review of the approved strategies and policies to ensure they remain effective and aligned with SCML's objectives.

7.2. Board-level IT Strategy Committee (ITSC)

7.2.1. The Board shall oversee the ITSC, which shall be responsible for:

7.2.1.1. Ensuring SCML has a robust IT strategic planning process in place.

7.2.1.2. Guiding the preparation of the IT Strategy to ensure alignment with the overall strategy of SCML for achieving business goals.

7.2.1.3. Ensuring that the IT Governance and Information Security Governance structures promote accountability, effectiveness, and efficiency, with adequately skilled resources, well-defined objectives, and clear responsibilities at all organizational levels.

7.2.1.4. Confirming that processes are established for assessing and managing IT and cybersecurity risks effectively.

7.2.1.5. Ensuring that budget allocations for the IT function (including IT security and cybersecurity) are

commensurate with SCML's IT maturity, digital capabilities, threat landscape, and industry standards, and that they are utilized effectively to meet stated objectives.

7.2.2. Reviewing the adequacy and effectiveness of SCML's Business Continuity Planning and Disaster Recovery Management at least annually.

7.3. Senior Management

7.3.1. The Senior Management of SCML is responsible for ensuring the efficient and secure functioning of the IT systems and processes. Key responsibilities include:

7.3.1.1. Implementing the IT Strategy as approved by the Board of Directors, ensuring alignment with business objectives.

7.3.1.2. Ensuring that IT and Information Systems (IS), along with their support infrastructure, are operating efficiently and effectively, enabling seamless business operations.

7.3.1.3. Establishing and maintaining robust IT risk management processes, promoting a culture of risk awareness, and fostering cyber hygiene practices across SCML.

7.3.1.4. Ensuring that SCML's cybersecurity posture is strong, proactive, and capable of mitigating emerging threats and vulnerabilities.

7.3.1.5. Ensuring that IT enhances productivity, effectiveness, and efficiency throughout SCML, thereby driving overall business performance.

7.4. Senior Management Level- IT Steering Committee

7.4.1. The IT Steering Committee is responsible for ensuring the alignment of IT activities with the overall business

strategy and maintaining the efficiency and security of IT operations. Key responsibilities include:

7.4.1.1. Assisting the IT Strategy Committee (ITSC) in formulating strategic IT plans and ensuring that IT performance is aligned with SCML's business objectives.

7.4.2. Overseeing the implementation and effectiveness of processes related to business continuity and disaster recovery, ensuring SCML's readiness for any IT-related disruptions.

7.4.3. Ensuring that a robust IT architecture is in place, meeting all statutory, regulatory, and security requirements, and is capable of supporting SCML's growth and technological needs.

7.4.4. Regularly updating the ITSC and the Managing Director on the progress, activities, and performance of the IT Steering Committee, ensuring transparency and accountability.

7.5. Board-Level Risk Management Committee

7.5.1. The Risk Management Committee of the Board (RMCB) plays a critical role in overseeing the management of risks associated with IT and cybersecurity within SCML.

7.5.2. The committee is responsible for ensuring that all potential risks are identified, assessed, and mitigated in alignment with SCML's business objectives and regulatory requirements.

7.5.3. Conducting at least an annual review, in consultation with the IT Strategy Committee (ITSC), to evaluate and update the IT related risks in risk management policy.

7.6. Information Security Committee (ISC)

7.6.1. The Information Security Committee (ISC) plays a pivotal role in safeguarding SCML's information assets and mitigating cybersecurity risks. The committee's responsibilities, inter alia, include:

7.6.1.1. Formulating and overseeing the implementation of information and cybersecurity policies, standards, and procedures.

7.6.1.2. Ensuring that all identified risks are managed within SCML's risk appetite and aligned with the overall risk management framework.

7.6.1.3. Approving and monitoring the progress of information security projects and initiatives to ensure effective implementation.

7.6.1.4. Leading efforts to enhance cybersecurity awareness across SCML through training and awareness campaigns.

7.6.1.5. Reviewing and analyzing cyber incidents, conducting post-incident evaluations, and ensuring appropriate corrective measures are in place.

7.6.1.6. Monitoring information systems audit findings and observations, ensuring timely mitigation of identified vulnerabilities.

7.6.1.7. Providing periodic updates to the ITSC and the Managing Director on key information security activities, risks, projects, and incident management efforts.

7.7. Head of IT Function (CTO/CIO)

7.7.1. The Head of IT Function plays a crucial role in ensuring that the IT infrastructure and processes support the overall strategy and operations of SCML. The responsibilities include, inter alia:

7.7.1.1. Ensuring that the execution of all IT projects and initiatives aligns with SCML's IT Policy and overall IT Strategy, facilitating the achievement of business objectives.

7.7.1.2. Establishing and maintaining an effective organizational structure that supports IT functions across SCML, ensuring efficiency in IT operations and support.

7.7.1.3. Developing, implementing, and managing a robust disaster recovery setup and business continuity strategy to minimize operational disruptions and ensure resilience in the face of unexpected events.

7.7.2. The Head of IT Function acts as the first line of defence by ensuring thorough assessment, evaluation, and management of IT controls and IT risks. They shall Implement robust internal controls to:

7.7.2.1. Secure SCML's information assets.

7.7.2.2. Ensure compliance with internal policies, regulatory mandates, and legal requirements related to IT operations.

7.8. Chief Information Security Officer (CISO)

7.8.1. The Chief Information Security Officer (CISO) holds a critical role in maintaining and enhancing the cybersecurity posture of SCML. The responsibilities include, at a minimum:

7.8.1.1. The CISO is responsible for formulating and driving the overall cyber security strategy of SCML.

7.8.1.2. Ensures compliance with all regulatory and statutory requirements related to information and cyber security.

7.8.1.3. Enforces SCML's policies designed to protect its information assets, ensuring that they are in line with the cybersecurity framework.

7.8.1.4. Acts as the central coordinator for all information and cybersecurity-related issues within SCML and with relevant external agencies.

7.8.1.5. The CISO is a permanent invitee to ITSC and the IT Steering Committee, providing input on cybersecurity aspects and aligning SCML's strategy with regulatory expectations.

7.8.1.6. The CISO's Office is responsible for managing and monitoring the Security Operations Centre (SOC) and overseeing the execution of cybersecurity-related projects to ensure comprehensive coverage of SCML's security needs.

7.8.1.7. Ensures that all deployed security solutions within SCML are functioning effectively and efficiently, mitigating risks associated with cyber threats.

7.8.1.8. The CISO directly reports to the Executive Director or an equivalent executive who oversees SCML's risk management function, ensuring that cybersecurity issues are elevated to the top levels of management.

7.8.1.9. The CISO is responsible for placing a quarterly review of the cybersecurity risks, arrangements, and preparedness of SCML before the Board of Directors, RMCB, and ITSC.

7.9. Audit Committee of the Board

7.9.1. The Audit Committee of the Board (ACB) plays a crucial role in overseeing the information systems (IS) audit function within SCML.

7.9.2. The ACB is responsible for ensuring that the IS audit processes are robust, independent, and aligned with the regulatory guidelines.

7.9.3. This oversight ensures that SCML's IT systems, information security framework, and cyber resilience measures are compliant with internal policies, legal requirements, and industry standards.

8. IT Service Management Framework

8.1. SCML establishes and maintains a comprehensive IT Services Management Framework to ensure the operational resilience, efficiency, and continuity of its IT systems and infrastructure, including disaster recovery (DR) capabilities.

8.2. This framework applies to all IT services, including software, hardware, information systems, and the supporting infrastructure within SCML.

8.3. SCML implements a robust IT Service Management Framework to support and manage its information systems and infrastructure. This framework ensures the operational resilience of the entire IT environment, including primary and disaster recovery (DR) sites, in line with SCML's business continuity objectives.

8.4. A Service Level Management process is established to manage IT operations effectively. The SLM ensures clear segregation of duties, operational efficiency, and the monitoring of service delivery standards to meet business requirements.

8.5. SCML identifies and classifies all information assets based on their Confidentiality, Integrity, and Availability. This classification is aligned with SCML's operations and the criticality of these assets to ensure adequate protection and management. The classification standards shall comply with SCML's **Information Asset Policy**.

8.6. To ensure the uninterrupted functioning of business operations, SCML avoids the use of outdated or unsupported hardware and software. SCML implements processes for continuous monitoring of software end-of-support (EOS) dates and the Annual Maintenance Contract (AMC) status of all IT hardware. Timely renewals and updates be ensured to prevent operational disruptions.

8.7. SCML develops and maintains a Technology Refresh Plan to ensure the timely replacement of hardware and software before they reach their EOS. This plan prioritizes business-critical infrastructure and ensure compliance with industry best practices and regulatory requirements.

8.8. SCML's standards for hardware and software, including security requirements, upgrade cycles, and usage guidelines, are clearly defined in the **Information Asset Policy**. All IT services management processes adhere strictly to these standards to ensure the integrity and reliability of the IT environment.

9. Outsourcing Arrangements

9.1. SCML establishes and maintains a comprehensive framework for managing outsourcing arrangements in the Information Technology (IT) and Cyber Security ecosystems, ensuring that risks associated with third-party services are effectively mitigated and aligned with SCML's overall risk management strategy.

9.2. This clause applies to all outsourcing arrangements within the IT and Cyber Security ecosystem, distinguishing between services that fall under the applicability of the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023, and those that do not.

9.3. For all outsourcing arrangements that fall under the applicability of the *Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023*, SCML shall ensure compliance with the guidelines specified therein. SCML has implemented a separate **IT Outsourcing Policy** that details the processes, controls, and reporting mechanisms required to manage such outsourced services, including vendor due diligence, contract management, performance monitoring, and regulatory reporting.

9.4. For outsourcing arrangements that are not governed by the *Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023*, SCML establishes a Vendor Risk Assessment Process. This process, proportionate to the assessed risk and materiality of the outsourced service, shall be documented as specified in SCML's **IT Outsourcing Policy**. The process shall include, but not be limited to, the following controls:

9.4.1. Mitigating Concentration Risk

9.4.2. Addressing Conflict of Interests

9.4.3. Mitigating Single Point of Failure

9.4.4. Compliance with Legal and Regulatory Requirements

9.4.5. Ensuring High Availability

9.4.6. Supply Chain Risk Management

9.5. SCML shall periodically review its outsourcing arrangements and vendor risk assessment processes to ensure alignment with evolving business requirements, regulatory changes, and industry best practices. Regular updates to the IT Outsourcing Policy shall be made as necessary.

10. Capacity Management of IT Resources

10.1. SCML ensures that its IT systems and supporting infrastructure are adequately equipped to handle business

functions and ensure uninterrupted service delivery across all channels.

10.2. The availability of IT resources is continuously monitored to prevent disruptions or performance degradation.

10.3. SCML conducts a proactive assessment of its IT capacity requirements on an annual basis, or more frequently if needed.

10.4. This assessment covers all critical components, including hardware, software, services, system resources, and supporting infrastructure. The capacity planning shall account for

10.4.1. Past trends (e.g., peak usage patterns),

10.4.2. Current business requirements, and,

10.4.3. Projected future needs based on SCML's IT strategy and growth plans.

10.5. IT capacity planning is consistent with SCML's strategic objectives, ensuring alignment with long-term business goals and scalable for future expansion.

10.6. The IT Strategy Committee (ITSC) shall periodically review the assessment of IT capacity requirements and the measures taken to address capacity issues. Any gaps, improvements, or enhancements identified during the assessment process shall be actioned upon to ensure continuous operational readiness.

11. IT Project Management Framework

11.1. SCML adopts a consistent and formally defined project management framework for all IT initiatives. This framework incorporates:

11.1.1. Active stakeholder involvement at key stages,

11.1.2. Ensuring effective oversight, monitoring, and management of project risks,

11.1.3. Timelines and progress.

11.2. In the adoption of new technologies, tools, or upgrades to existing systems, SCML shall adhere to a standardized enterprise planning methodology. This approach will ensure that all technological advancements are aligned with SCML's overall business and IT strategies, fostering secure, resilient, and efficient information sharing across the Company.

11.3. SCML shall ensure that the adoption of any new or emerging technologies is proportional to its Risk appetite and aligns with its business and IT strategy. This approach shall ensure the optimal use and protection of information assets while maintaining the security and resilience of the technology environment.

11.4. To ensure data consistency and facilitate efficient data sharing among various applications and systems, SCML maintains an enterprise data dictionary. This will provide a common understanding of data across SCML, promoting seamless integration across information systems.

11.5. SCML ensures that formal agreements with software vendors are in place to provide continuous maintenance and support for all critical applications. These agreements shall ensure that the necessary updates, patches, and program fixes are regularly applied, thereby maintaining the operational integrity of essential software.

11.6. For critical applications, SCML obtains the source code from the vendor whenever feasible. In cases where this is not possible, SCML shall implement a Source code escrow arrangement or other risk mitigation mechanisms to safeguard against vendor default. These arrangements shall ensure access to essential product updates and fixes when required.

11.7. SCML secures a certificate or formal confirmation from the application developer or vendor, verifying that the application is free from known vulnerabilities, malware, or covert channels in the code. This certification shall be renewed with any material changes, such as upgrades or significant modifications to the application.

11.8. Before implementing any new IT application as a business product, SCML shall subject the application to a formal product approval and quality assurance process. This process shall ensure that the application meets SCML's security, performance, and operational standards.

12. Change & Patch Management

12.1. SCML implements and maintain a separate **Change and Patch Management Policy**, which outlines documented procedures to manage changes and patches effectively, ensuring:

12.1.1. Any patches or changes to systems, applications, or data are assessed for their business impact. This includes evaluating the potential consequences of both implementing and not implementing the patch or change request, ensuring alignment with business goals.

12.1.2. Patches and changes shall be applied or implemented securely and within an appropriate timeframe. All changes shall be reviewed and approved through the established processes to ensure security and compliance.

12.1.3. Any modification to an application system or data shall be driven by legitimate business needs. All changes shall be documented, justified, and subject to a robust

change management process, requiring necessary approvals.

12.1.4. SCML shall establish mechanisms to recover from failed changes, unsuccessful patch deployments, or any unintended outcomes, ensuring minimal disruption to operations.

12.2. The **Change and Patch Management Policy** serves as the guiding framework for the secure and controlled management of changes and patches across SCML's IT environment.

13. Data Migration/Transfer Mechanism

13.1. SCML establishes and maintain a comprehensive **Data Migration/Transfer Policy** to govern the systematic process of data migration, ensuring data integrity, completeness, and consistency throughout the transfer process. This policy encompasses the following key elements:

13.1.1. The policy includes provisions for obtaining necessary signoffs from business users and application owners at each stage of the migration process, ensuring accountability and agreement on data handling.

13.1.2. Comprehensive audit trails are maintained throughout the migration process to track changes, monitor compliance, and facilitate traceability of data movements and modifications.

13.1.3. To prevent unauthorized modifications of data, SCML ensures that there is no manual intervention or manual modification of data while it is being transferred from one process to another or from one application to another for critical applications.

13.1.4. The data transfer mechanism between processes or applications is thoroughly tested and securely automated, incorporating necessary checks and

balances. This process is integrated using the Straight Through Processing methodology, with appropriate authentication mechanisms and audit trails in place to safeguard the integrity of the data being transferred.

14. Audit Trails & System Logging

14.1. All IT applications within SCML that handle or influence critical or sensitive information shall have built-in capabilities for generating detailed audit trails and maintaining system logs, ensuring thorough tracking and visibility of system activities.

14.2. The audit trails satisfies both SCML's operational needs and all relevant regulatory and legal requirements. These records are comprehensive enough to:

14.2.1. Facilitate internal audits,

14.2.2. Serve as forensic evidence when necessary, and,

14.2.3. Assist in resolving disputes, particularly in supporting non-repudiation.

14.3. SCML implements a system for continuously monitoring audit trails and system logs to promptly identify and address any unauthorized activities or security breaches. This monitoring system is critical for ensuring the integrity and security of SCML's information systems.

15. Cryptographic Standards

15.1. SCML ensures that all cryptographic controls used for data transmission, processing, and authentication are robust and in line with internationally recognized and published standards. This includes but is not limited to the use of strong key lengths, secure algorithms, cipher suites, and applicable protocols.

15.2. SCML ensures that these standards are not deprecated, compromised, or demonstrated to be insecure.

15.3. All configurations associated with implementing cryptographic controls strictly complies with prevailing laws, regulatory guidelines, and industry best practices to ensure the security and integrity of sensitive information.

16. Physical & Environmental Security Controls

16.1. SCML implements robust physical and environmental security controls at both their Data Centres (DC) and Disaster Recovery (DR) sites to safeguard critical IT infrastructure.

16.2. The DC and DR sites is located in geographically distinct areas to ensure that both sites are not vulnerable to the same location-specific threats, such as natural disasters or regional outages.

16.3. SCML establishes and maintains appropriate E-surveillance mechanisms to continuously monitor and secure both the DC and DR sites against unauthorized access and potential security breaches.

16.4. SCML ensures that the DC and DR sites are equipped with essential physical and environmental controls, including but not limited to fire suppression systems, power backup, climate control, and secure access protocols to prevent physical damage or intrusion.

17. IT Access Control Measures

17.1. Access to SCML's information assets is granted solely based on valid business requirements.

17.2. SCML maintains a comprehensive IT Access Control Standards as specified in **Information Asset Policy**, approved by the ITSC, to administer and monitor access

rights. These standards and procedures shall be regularly updated to ensure compliance and effectiveness.

17.3. Personnel with elevated system access privileges shall be subject to close supervision, with all activities logged and periodically reviewed to prevent unauthorized or malicious actions.

17.4. SCML enforces multi-factor authentication (MFA) for privileged users accessing critical information systems and performing critical tasks, as determined by a risk assessment conducted by the company.

17.5. In teleworking or remote work scenarios, SCML shall:

17.5.1. Ensure that all systems used remotely, and the connections established from alternate work locations to SCML's environment are secure.

17.5.2. Implement MFA for enterprise access to critical systems.

17.5.3. Maintain a mechanism to identify and monitor all remote-access devices connected to SCML 's systems.

17.5.4. Ensure that all data and information shared or accessed during teleworking is secured appropriately.

18. IT Performance and Metrics

18.1. SCML establishes appropriate metrics to monitor and evaluate the performance, recovery, and business resumption capabilities of all critical information systems. These metrics includes, but is not limited to, Recovery Point Objective (RPO) and Recovery Time Objective (RTO), ensuring minimal data loss and downtime during any disruption.

18.2. For non-critical information systems, SCML adopts a risk-based approach to determine suitable performance and recovery metrics, ensuring that resources are allocated in proportion to the level of risk posed by each system.

18.3. SCML implements a structured methodology or scorecard system to measure IT performance, operational efficiency, and IT maturity levels. This framework shall provide clear and actionable insights into SCML 's overall IT health and areas for improvement.

19. Information Security Management Framework

19.1. SCML is committed to ensuring the confidentiality, integrity, and availability of its information assets through a comprehensive Information Security Management Framework.

19.2. The framework is designed to mitigate risks associated with information security threats and vulnerabilities, ensuring protection from unauthorized access, disclosure, alteration, or destruction of information.

19.3. SCML has a separate, detailed **Information Security Policy**, which outlines specific guidelines, procedures, and responsibilities for safeguarding information assets. All personnel are required to adhere to the stipulations set forth in this policy to ensure a secure operating environment.

19.4. The Information Security Management Framework includes regular assessments of potential risks, implementation of preventive and detective controls, and continuous monitoring of security incidents. These measures are designed to identify and address any gaps in the security infrastructure, ensuring timely responses to any identified threats.

19.5. To maintain the highest levels of information security, the framework incorporates ongoing training and awareness programs for all employees.

20. Cyber Security Management Framework

20.1. SCML is dedicated to safeguarding its digital assets and critical information systems through a robust Cyber Security Management Framework. This framework is designed to protect SCML from evolving cyber threats, ensuring the confidentiality, integrity, and availability of its data and IT infrastructure.

20.2. SCML has a separate **Cyber Security Policy**, which includes detailed provisions on the **Cyber Crisis Management Plan (CCMP)/Cyber Incident Response Plan & Recovery Management Plan**. These policies outline the protocols for identifying, responding to, and recovering from cyber incidents, ensuring that SCML can quickly and efficiently mitigate the impact of any security breach.

20.3. In the event of a cyber incident, the framework ensures swift and effective containment, investigation, and remediation, minimizing damage and ensuring business continuity.

20.4. To reinforce cybersecurity awareness, the framework mandates regular training and drills for all employees on cyber threat identification and response. Additionally, all third-party vendors and partners are required to comply with the SCML's cybersecurity standards, ensuring the protection of data across the extended supply chain.

20.5. Any changes in the cyber environment are managed through a formal change and patch management process to prevent new vulnerabilities from arising.

21. Risk Assessment Framework

21.1. SCML implements a comprehensive risk assessment process for all information assets within its operational scope, guided by internationally recognized security standards and IT control frameworks. This risk assessment ensures the

identification, evaluation, and mitigation of risks associated with information systems, aligning with SCML 's overall risk management strategy.

21.2. All employees, contractors, and service providers comply with SCML's information security policies and acceptable-use guidelines. This requirement extends to external parties accessing SCML's systems and data, ensuring that they adhere to the same high standards of security.

21.3. SCML reviews its security infrastructure and policies on an annual basis, factoring in both internal experiences and emerging threats, such as phishing, spoofing, and other cyberattacks. Steps shall be taken to proactively prevent, detect, and mitigate these threats, ensuring resilience against evolving cyber risks.

21.4. SCML's **Risk Management Policy** incorporates IT-related risks, including cybersecurity risks, and the Risk Management Committee of the Board (RMCB), in consultation with the Information Technology Strategy Committee (ITSC), shall periodically review and update the policy at least once a year to adapt to new challenges and

22. Vulnerability Assessment (VA)/Penetration Testing (PT)

22.1. SCML implements a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) procedure to identify and mitigate security weaknesses across its IT infrastructure and applications.

22.2. The VA & PT involves regular assessments of critical systems, applications, and networks to ensure they are protected against emerging threats and vulnerabilities. The objective is to proactively detect potential security gaps and address them before they can be exploited by malicious actors.

22.3. All VA & PT activities is conducted in line with industry standards and best practices, using a combination of automated tools and manual techniques. The assessments will be performed by qualified internal teams or external experts, ensuring an unbiased and thorough evaluation of SCML's security posture. Remediation of identified vulnerabilities shall be prioritized based on their severity and potential impact, with progress tracked through regular reporting and review.

22.4. SCML has a separate **Vulnerability Assessment and Penetration Testing Policy** that outlines detailed procedures, methodologies, and roles and responsibilities for conducting VA & PT.

22.5. To maintain a robust security environment, SCML conducts VA & PT exercises at regular intervals or whenever significant changes occur in the IT environment, such as system upgrades or new deployments.

23. Business Continuity and Disaster Recovery Management

23.1. SCML is committed to ensuring business continuity and disaster recovery through a well-structured Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). These plans are designed to minimize the impact of disruptions to critical business functions and IT services, ensuring that essential operations can continue and recover swiftly in the event of unforeseen incidents such as natural disasters, cyber-attacks, or other emergencies.

23.2. The BCP & DRP framework involves identifying key business functions, critical IT infrastructure, and potential risks that could impact continuity.

23.3. SCML conducts regular risk assessments and business impact analyses to ensure that recovery strategies and solutions remain effective and up to date.

23.4. SCML has a separate **BCP (including DRP) Policy**, which details the specific procedures and responsibilities for activating and executing recovery operations. This serves as a comprehensive guide for SCML's response to different types of disruptions and is designed to align with industry best practices and regulatory requirements.

23.5. SCML will review and update the BCP & DRP at least annually, or whenever there are significant changes to the business or IT environment.

24. Information System (IS) Audit

24.1. SCML conducts regular Information System (IS) Audits to ensure that its IT infrastructure, applications, and processes are secure, compliant, and operating effectively.

24.2. The audits focus on evaluating the security controls, data integrity, and performance of SCML's IT systems, ensuring alignment with industry best practices and regulatory requirements. The IS Audit serves as a critical tool in identifying gaps and areas for improvement in the IT environment, enhancing overall system resilience.

24.3. The IS Audit process is carried out by qualified internal auditors or independent third-party auditors, depending on the nature and complexity of the systems being audited. The audit scope shall cover all critical information assets, including databases, network architecture, access controls, and data processing mechanisms. Findings from the IS Audit is documented in detailed audit reports, and any identified issues shall be addressed through corrective actions, with progress tracked and reviewed Audit Committee of the Board.

24.4. SCML has a separate **Information System (IS) Audit Policy**, which provides comprehensive guidelines and procedures for conducting audits. The Policy ensures that audits are conducted in a structured and consistent manner, aligning with SCML's overall risk management framework and regulatory compliance requirements.

24.5. To maintain a robust information security posture, the IS Audit shall be conducted at least annually or more frequently if required due to significant changes in the IT environment.

25. Approval, Review & Update

25.1. This policy is approved by the Board and reviewed at least once a year or as and when there are any changes introduced as per the guidelines/ directions issued by RBI or as and when it is found necessary to change the policy due to business needs.