



# **OPERATIONAL RISK MANAGEMENT MODULE**

CONSULTATION



<b>MODULE</b>	<b>OM Operational Risk Management</b>
	<b>Table of Contents</b>

	<b>Date Last Changed</b>
<b>OM-A Introduction</b>	
OM-A.1 Purpose	03/2019
OM-A.2 [This Chapter was deleted in October 2007]	10/2007
OM-A.3 Module History	03/2019
<b>OM-B General Guidance and Best Practice</b>	
OM-B.1 [This Section was moved to Chapter OM-1]	10/2007
<b>OM-1 Procedures International Guidance and Best Practice</b>	
OM-1.1 [This Chapter was deleted in March 2019]	10/2012
<b>OM-2 General Requirements</b>	
OM-2.1 Operational Risk Management Framework	03/2019
OM-2.2 [This Chapter was deleted in March 2019]	07/2011
OM-2.3 [This Chapter was deleted in March 2019]	10/2007
OM-2.4 Succession Planning	03/2019
<b>OM-3 Outsourcing</b>	
OM-3.1 Introduction	03/2019
OM-3.2 Supervisory Approach	03/2019
OM-3.3 Notifications and Prior Approval	03/2019
OM-3.4 Risk Assessment	03/2019
OM-3.5 Outsourcing Agreement	03/2019
OM-3.6 Contingency Planning for Outsourcing	03/2019
OM-3.7 [This Section was deleted in March 2019 and requirements were moved to Chapter HC-6.5]	10/2015
OM-3.8 Intra-group Outsourcing	03/2019
OM-3.9 Outsourcing of Functions Containing Customer Information	03/2019
<b>OM-4 Electronic Money and Electronic Banking Activities</b>	
OM-4.1 Electronic Banking	03/2019



<b>MODULE</b>	<b>OM Operational Risk Management Table of Contents (continued)</b>
---------------	---

		<b>Date Last Changed</b>
<b>OM-5</b>	<b>Business Continuity Planning</b>	
OM-5.1	Introduction	03/2019
OM-5.2	General Requirements	10/2012
OM-5.3	Board and Senior Management Responsibilities	03/2019
OM-5.4	Developing a Business Continuity Plan	03/2019
OM-5.5	BCP – Recovery Levels & Objectives	07/2011
OM-5.6	Detailed Procedures for the BCP	07/2011
OM-5.7	Vital Records Management	07/2011
OM-5.8	Other Policies, Standards and Processes	03/2019
OM-5.9	Maintenance, Testing and Review	03/2019
OM-5.10	Cyber Security Risk Management	03/2019
<b>OM-6</b>	<b>Security Measures for Banks</b>	
OM-6.1	Physical Security Measures for Retail Banks	03/2019
OM-6.2	Internet Security for all Banks	04/2016
OM-6.3	ATM Security Measures: Hardware/Software for Retail Banks	03/2019
OM-6.4	ATM Security Measures: Physical Security for Retail Banks	03/2019
OM-6.5	ATM Security Measures: Additional Measures for Retail Banks	04/2016
OM-6.6	Cyber Security Measures	12/2019
	<b>Books and Records</b>	
<b>OM-7</b>		
OM-7.1	General Requirements	10/2011
OM-7.2	Transaction Records	07/2017
OM-7.3	Other Records	04/2011
	<b>Qualitative Aspects</b>	
<b>OM-8</b>		
OM-8.1	[This Section was deleted in March 2019 and requirements are now covered under Chapter OM-2].	10/2012
OM-8.2	[This Section was deleted in March 2019 and requirements are now covered under Chapter OM-2].	10/2012
OM-8.3	Standardised Approach	10/2012
	<b>APPENDICES</b>	
	Appendix A: Loss Event Type Classification	03/2019
	Appendix B: Cyber Security Control Guidelines	12/2019



MODULE	OM: Operational Risk Management
CHAPTER	OM-6 Security Measures for Banks

## OM-6.6 Cyber Security Risk Management

### *Role of the Board*

**OM-6.6.1** The Board of conventional bank licensees must ensure that the bank has a robust cyber security risk management framework to comprehensively manage the bank's cyber security risk and vulnerabilities. The Board must establish clear ownership and management accountability for risks associated with cyber-attacks and related risk management and recovery processes. Cyber security must be an item for discussion at Board meetings.

**OM-6.6.2** The Board of conventional bank licensees must ensure that the cyber security risk management framework encompasses, at a minimum, the following components:

- Cyber security strategy;
- Cyber risk management policy; and
- Cyber security risk management approach, tools and methodology.

**OM-6.6.3** Boards should receive comprehensive reports covering cyber security issues such as the following:

- Key Risk Indicators/ Key Performance Indicators;
- Status reports on overall cyber security control maturity levels;
- Updates on latest internal or relevant external cyber security incidents; and
- Results from penetration testing exercises.

**OM-6.6.4** The Board must ensure that it approves the cyber security risk management framework which must be evaluated by it for scope coverage, adequacy and effectiveness on an annual basis, taking into account emerging cyber threats and credible benchmarks for cyber security controls.

**OM-6.6.5** The Board of banks that are identified as being exposed to material cyber security risks must take measures to establish a cyber security risk management function, independent of the technology (IT) department, which must report to an independent risk management function or an equivalent function within the bank. The cyber security risk management function must monitor and report on the status and maturity of all relevant cyber security controls.



MODULE	OM: Operational Risk Management
CHAPTER	OM-6: Security Measures for Banks

## OM-6.6 Cyber Security Risk Management

### *Role of Senior Management*

OM-6.6.6 The senior management must be responsible for the following activities:

- (a) Create the overall cyber security risk management framework and adequately oversee its implementation;
- (b) Formulate a bank-wide cyber security strategy and cyber risk management policy;
- (c) Implement and consistently maintain an integrated, bank-wide, cyber security risk management framework, including sufficient resource allocation;
- (d) Monitor the effectiveness of the implementation of cyber security risk management practices and coordinate cyber security activities with internal and external risk management entities;
- (e) Provide periodic reports to the Board on the current situation with respect to cyber threats and cyber security risk treatment;
- (f) Prepare periodic reports on all cyber incidents (internal and external) and their implications on the bank; and
- (g) Ensure that processes for identifying the cyber risk levels of internal functions are in place and annually evaluated.

OM-6.6.7 The senior management must ensure that:

- (a) The bank has identified clear internal ownership and classification for all information assets and data;
- (b) The bank has maintained an inventory of the information assets and data which is reviewed and updated regularly;
- (c) The cyber security staff are adequate to manage the bank's cyber security risks and facilitate the performance and continuous improvement of all relevant cyber security controls;
- (d) It provides and requires cyber security staff to attend regular cyber security update and training sessions; and
- (e) It requires key cyber security staff to take steps to stay abreast of changing cyber security threats and countermeasures.

OM-6.6.8 [The requirements included in this Paragraph are now included in paragraph OM-6.6.35.]



MODULE	OM: Operational Risk Management
CHAPTER	OM-6: Security Measures for Banks

## OM-6.6 Cyber Security Risk Management (Continued)

### *Cyber Security Strategy*

- OM-6.6.9 A bank-wide cyber security strategy must be defined and documented to include:
- The position and importance of cyber security at the bank;
  - The primary cyber security threats and challenges facing the bank;
  - The bank's approach to cyber risk management;
  - The key elements of the cyber security strategy including objectives, principles of operation and implementation approach;
  - Scope of risk identification and assessment, which must include the dependencies on third party service providers;
  - Approach to planning response and recovery activities; and
  - Approach to communication with internal and external stakeholders including sharing of information on identified threats and other intelligence among industry participants.

OM-6.6.10 The cyber security strategy should be communicated to the relevant stakeholders and it should be revised as necessary and, at least, once every three years. Appendix B provides cybersecurity control guidelines that can be used as reference to support the bank's cybersecurity strategy and cybersecurity policy.

### *Cyber Security Risk Policy*

- OM-6.6.11 Conventional bank licensees must implement a written cyber security risk management setting forth its policies for the protection of its electronic systems and client data stored on those systems, which must be reviewed and approved by the licensee's board of directors or senior management, as appropriate, at least annually. The cyber security policy must address the following areas:
- Definition of the key cyber security functions within the bank, the roles which will have responsibility and accountability for these functions, and a clear communication plan to the Board on the status and maturity of the key cyber security functions.
  - A statement of the bank's overall cyber risk tolerance as aligned with the bank's business strategy. The cyber risk tolerance statement should be developed through consideration of the various impacts of cyber threats including customer impact, service downtime, potential negative media publicity, potential regulatory penalties, financial loss, and others;
  - Definition of main cyber security processes and measures and the approach to control and assessment;



ODULE	OM: Operational Risk Management
CHAPTER	OM-6: Security Measures for Banks

## OM-6.6 Cyber Security Risk Management (Continued)

- (d) Policies and procedures (including process flow diagrams) for all relevant cyber security functions and controls including the following:
- (a) Asset management (Hardware and software);
  - (b) Incident management (Detection and response);
  - (c) Vulnerability management;
  - (d) Configuration management;
  - (e) Access management;
  - (f) Third party management;
  - (g) Secure application development;
  - (h) Secure change management;
  - (i) Cyber training and awareness;
  - (j) Cyber resilience (business continuity and disaster planning); and
  - (k) Secure network architecture.

### *Approach, Tools and Methodology*

OM-6.6.12 Conventional bank licensees must ensure that the cyber security policy is effectively implemented through a consistent approach using tools and methodologies that are commensurate with the size and risk profile of the bank. The approach, tools and methodologies must cover all cyber security functions and controls defined in the cyber security policy.

### *Prevention Controls*

OM-6.6.13 A conventional bank licensee must develop and implement preventive measures across all relevant technologies to minimise the bank's exposure to cyber security risk. Such preventive measures must include, at a minimum, the following:

- (a) Deployment of anti-virus software and anti-malware programme to detect, prevent, and isolate malicious code;
- (b) Data leakage prevention solutions to detect and prevent confidential data from leaving the bank's technology environment;
- (c) Use of firewalls for network segmentation and access control lists to limit unauthorized system access between network segments;
- (d) Rigorous security testing at software development stage to limit the number of vulnerabilities;
- (e) Use of authority matrices to limit privileged internal and external access rights to systems and data;



- (f) Use of a secure email gateway to limit email based cyber attacks such as malware attachments, malicious links, and phishing scams;

MODULE	OM: Operational Risk Management
CHAPTER	OM-6: Security Measures for Banks

## OM-6.6 Cyber Security Risk Management (Continued)

- (g) Use of a web gateway to limit browser based cyber attacks and malicious websites;
- (h) Use of mobile device management solutions to secure all mobile devices with any access to bank systems, applications, and networks through security measures such as encryption, remote wipe capabilities, and password enforcement. Network access control to secure physical network ports against connection to computers which are unauthorised to connect to the bank's network or which do not meet the minimum security requirements defined for bank computer systems; and
- (i) Identity and access management solutions to limit the exploitation and monitor the use of privileged and non-privileged accounts.

### *Cyber Risk Identification and Assessments*

OM-6.6.14 Conventional bank licensees must conduct periodic assessments of cyber threats. For the purpose of analysing and assessing current cyber threats relevant to the bank, it should take into account the factors detailed below:

- (a) Cyber threat entities including cyber criminals, cyber activists, insider threats;
- (b) Methodologies and attack vectors across various technologies including cloud, email, websites, third parties, physical access, or others as relevant;
- (c) Changes in the frequency, variety, and severity of cyber threats relevant to the region;
- (d) Examples of cyber threats from past cyber attacks on the bank if available; and
- (e) Examples of cyber threats from recent cyber attacks on other organisations.

OM-6.6.15 Conventional bank licensees must conduct periodic assessments of the maturity, coverage, and effectiveness of all cyber security controls. Cyber security control assessment must include an analysis of the controls' effectiveness in reducing the likelihood and probability of a successful attack.





OM-6.6.16 Banks should ensure adequate coverage of the periodic threat assessments and cyber security controls ensuring all technology systems are included. A risk treatment plan must be developed for all residual risks which are considered to be above the bank's risk tolerance levels.

CONSULTATION



MODULE	OM: Operational Risk Management
CHAPTER	OM-6: Security Measures for Banks

## OM-6.6 Cyber Security Risk Management (Continued)

### *Vulnerability Management*

**OM-6.6.17** Conventional bank licensees must conduct regular technical assessments to identify potential security vulnerabilities for systems, applications, and network devices. The vulnerability assessments must be comprehensive and cover internal technology, external technology, and connections with third parties.

**OM-6.6.18** Conventional bank licensees must ensure that the vulnerabilities identified are addressed and that security patches are applied where relevant within a timeframe that is commensurate with the risks posed by each vulnerability.

**OM-6.6.19** All banks must regularly perform internal and external penetration testing of their systems, applications, and network devices to verify the robustness of the security controls in place. These tests must be used to simulate real world cyber attacks on the technology environment and must:

- (a) Follow an internationally recognized methodology, such as National Institute of Standards and Technology “NIST” and Open Web Application Security Project “OWASP”;
- (b) Include both White Box and Black Box testing in its scope;
- (c) Be conducted by qualified and experienced security professionals who are certified in providing penetration testing services;
- (d) Be performed by external, independent third parties;
- (e) Be performed on either the production environment or on non-production exact replicas of the production environment; and
- (f) Be defined to include both assessment of potential vulnerabilities as well as attempts to demonstrate whether the identified vulnerabilities are exploitable.

### *Cyber Incident Detection and Management*

**OM-6.6.20** Conventional bank licensees must implement a cyber security incident management system to ensure timely detection, response, and recovery for cyber security incidents.

**OM-6.6.21** Banks should consider the adequacy of the security information and incident management system, keeping in view it should receive data on a real time basis from all relevant systems, applications, and network devices including operational and business systems. The monitoring system should be capable of identifying indicators



of cyber incidents and initiate alerts, reports, and response activities based on the defined cyber security incident management process.

<b>MODULE</b>	<b>OM: Operational Risk Management</b>
<b>CHAPTER</b>	<b>OM-6: Security Measures for Banks</b>

## OM-6.6 Cyber Security Risk Management (Continued)

OM-6.6.22 Banks should determine the period of time necessary for retaining the information required for detecting cyber incidents, including "low-and-slow" attacks, in order to facilitate incident investigations.

**OM-6.6.23 Conventional bank licensees must regularly identify, test, review and update current cyber security risk scenarios and the corresponding response plan. This is to ensure that the scenarios and response plan remain relevant and effective, taking into account changes in the operating environment, systems or the emergence of new cyber security threats.**

OM-6.6.24 Banks should periodically review current cyber incident scenarios for the purpose of assessing the licensee's ability to detect and respond to these scenarios if they were to occur. If any gaps are identified, the security information and event management system should be updated with new use cases and rule sets which are capable of detecting the current cyber incident scenarios.

**OM-6.6.25 Conventional bank licensees must ensure that cyber security breaches detected are escalated to an incident response team, management and the Board, in accordance with the licensee's business continuity plan and crisis management plan, and that an appropriate response is implemented promptly (see also OM-6.6.35.)**

OM-6.6.26 For the purpose of managing a critical cyber incident, the licensee should operate a situation room, and should include in the incident management procedure a definition of the authorities and responsibilities of staff members, internal and external reporting lines, communication channels, tools and detailed working procedures.

OM-6.6.27 Banks should record and document in an orderly manner the incidents that have been handled and the actions that were taken by the relevant functions. In particular, the bank should maintain an "incident log" in which all the notifications, decisions and actions taken, in relation to cyber incidents, are documented, as close as possible to the time of their occurrence.

OM-6.6.28 Banks should determine the effects of the cyber incident on customers and to the wider banking system as a whole and report the results of such an assessment to the CBB if it is determined that the cyber incident may have a systemic impact.



MODULE	OM: Operational Risk Management
CHAPTER	OM-6: Security Measures for Banks

## OM-6.6 Cyber Security Risk Management (Continued)

### *Recovery*

**OM-6.6.29** Conventional bank licensees must identify the critical systems and services within its operating environment that must be recovered on a priority basis in order to provide certain minimum level of services during the downtime and determine how much time the bank will require to return to full service and operations.

**OM-6.6.30** Conventional bank licensees must define a program for recovery activities for timely restoration of any capabilities or services that were impaired due to a cybersecurity incident. Banks must establish recovery time objectives (“RTOs”), i.e. the time in which the intended process is to be covered, and recovery point objectives (“RPOs”), i.e. point to which information used must be restored to enable the activity to operate on resumption”. Banks must also consider the need for communication with third party service providers, customers and other relevant external stakeholders as may be necessary.

**OM-6.6.31** Conventional bank licensees must ensure that all critical systems are able to recover from a cyber security breach within the licensee’s defined RTO in order to provide important services or some level of minimum services for a temporary period of time.

**OM-6.6.32** Conventional bank licensees must define a program for exercising the various response mechanisms, taking into account the various types of exercises such as attack simulations, "war games" and "table top" exercises, and with reference to the relevant stakeholders such as technical staff, crisis management team, decision-makers and spokespersons.

**OM-6.6.33** Conventional bank licensees must define the mechanisms for ensuring accurate, timely and actionable communication of cyber incident response and recovery activities with the internal stakeholders, including to the board or designated committee of the board.

**OM-6.6.34** A conventional bank licensees must ensure its business continuity plan is comprehensive and includes a recovery plan for its systems, operations and services arising from a cyber security incident.



MODULE	OM: Operational Risk Management
CHAPTER	OM-6: Security Measures for Banks

## OM-6.6 Cyber Security Risk Management (Continued)

### *Cyber Security Insurance*

#### OM-6.6.35

Conventional bank licensees must arrange to seek cyber risk insurance cover from a suitable insurer, once the assessment of cyber security risk is complete. The insurance policy may include some or all of the following types of coverage, depending on the risk assessment outcomes:

- (a) Crisis management expenses, such as costs of notifying affected parties, costs of forensic investigation, costs incurred to determine the existence or cause of a breach, regulatory compliance costs, costs to analyse the insured's legal response obligations;
- (b) Claim expenses such as costs of defending lawsuits, judgments and settlements, and costs of responding to regulatory investigations; and
- (c) Policy also provides coverage for a variety of torts, including invasion of privacy or copyright infringement. First-party coverages may include lost revenue due to interruption of data systems resulting from a cyber or denial of service attack and other costs associated with the loss of data collected by the insured.

### *Red Teaming*

OM-6.6.36 The CBB may require additional red teaming exercises to be performed as needed. Where banks have been required to conduct a red teaming exercise the results of such an exercise must be provided to the CBB within one month of the completion of the report together with a comprehensive plan to address any observed weakness.

### *Training and Awareness*

OM-6.6.37 Conventional bank licensees must evaluate improvement in the level of awareness and preparedness to deal with cyber security risk to ensure the effectiveness of the training programmes implemented.

OM-6.6.38 The licensee must ensure that all employees receive adequate training on a regular basis, in relation to cyber security and the threats they could encounter, such as through testing employee reactions to simulated cyber attack scenarios. All relevant employees must be informed on the current cyber security breaches and threats. Additional training should be provided to 'higher risk staff'.



MODULE	OM: Operational Risk Management
CHAPTER	OM-6: Security Measures for Banks

## OM-6.6 Cyber Security Risk Management (Continued)

**OM-6.6.39** The conventional bank licensees must ensure that role specific cyber security training is provided on a regular basis to relevant staff including:

- (a) Executive board and senior management
- (b) Cyber security roles
- (c) Application developers and database administrators

### *Reporting to the CBB*

**OM-6.6.40** Conventional bank licensees must provide a preliminary report to the CBB on the day of the occurrence of any cyber incidents, whether internal or external, that compromises customer information or disrupts critical services that affect operations. If the day of the occurrence of the incident is unknown, then a preliminary report must be provided to the CBB on the day of detection and investigation. When reporting such instances, licensees must provide an initial root cause analysis of the cyber attack and current measures taken to ensure similar events do not reoccur.

**OM-6.6.41** Following the submission of the preliminary report on detection of a cyber security incident referred to in Paragraph OM-6.6.40, the licensee must submit to the CBB a comprehensive report within 5 working days of the occurrence of the cyber security incident. The comprehensive report must include all relevant details including the full root cause analysis of the cyber security incident and all measures taken by the licensee to ensure that similar events do not recur.

**OM-6.6.42** The penetration testing referred to in Paragraph OM-6.6.19, must be conducted at least twice per year.

**OM-6.6.43** The penetration testing report, along with the steps taken to mitigate the risks must be maintained by the bank for a five year period from the date of the report and must be provided to the CBB within two months following the end of the month where the testing took place, i.e. for a June test, the report must be submitted at the latest by 31<sup>st</sup> August and for a December test, by 28<sup>th</sup> February (see Section BR-4A.2).



## Appendix B – Cybersecurity Control Guidelines

The Control Guidelines consists of five Core Functions which are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

**Identify** – Develop a bank wide understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Cyber Security Risk Management Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables a bank to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

**Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity incident.

**Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity incident. The Detect Function enables timely discovery of cybersecurity events.

**Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

**Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Below is a listing of the specific cybersecurity activities that are common across all critical infrastructure sectors:

### **IDENTIFY**

**Asset Management:** The data, personnel, devices, systems, and facilities that enable the bank to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the bank's risk strategy.

1. Physical devices and systems within the bank are inventoried.
  2. Software platforms and applications within the bank are inventoried.
  3. Communication and data flows are mapped.
  4. External information systems are catalogued.
  5. Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
  6. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
-



**Business Environment:** The bank's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

1. Priorities for the bank's mission, objectives, and activities are established and communicated.
2. Dependencies and critical functions for delivery of critical services are established.
3. Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).

**Governance:** The policies, procedures, and processes to manage and monitor the bank's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

1. Bank's cybersecurity policy is established and communicated.
2. Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
3. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
4. Governance and risk management processes address cybersecurity risks.

**Risk Assessment:** The bank understands the cybersecurity risk to bank's operations (including mission, functions, image, or reputation), bank's assets, and individuals.

1. Asset vulnerabilities are identified and documented.
2. Cyber threat intelligence is received from information sharing forums and sources.
3. Threats, both internal and external, are identified and documented.
4. Potential business impacts and likelihoods are identified.
5. Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
6. Risk responses are identified and prioritized.

**Risk Management Strategy:** The bank's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

1. Risk management processes are established, managed, and agreed to by bank's stakeholders.
2. The bank's risk tolerance is determined and clearly expressed.
3. The bank's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

**Third Party Risk Management:** The bank's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing third party risk. The bank has established and implemented the processes to identify, assess and manage supply chain risks.

---





1. Cyber third party risk management processes are identified, established, assessed, managed, and agreed to by the bank's stakeholders.
2. Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber third party risk assessment process.
3. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an bank's cybersecurity program.
4. Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
5. Response and recovery planning and testing are conducted with suppliers and third-party providers.

## PROTECT

**Identity Management, Authentication and Access Control:** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

1. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
2. Physical access to assets is managed and protected.
3. Remote access is managed.
4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
5. Network integrity is protected (e.g., network segregation, network segmentation).
6. Identities are proofed and bound to credentials and asserted in interactions
7. Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

**Awareness and Training:** The bank's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

1. All users are informed and trained on a regular basis.
  2. Bank's security awareness programs are updated at least annually to address new technologies, threats, standards, and business requirements.
  3. Privileged users understand their roles and responsibilities.
  4. Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
  5. The Board and senior management understand their roles and responsibilities.
-



6. Physical and cybersecurity personnel understand their roles and responsibilities.
7. Software development personnel receive training in writing secure code for their specific development environment and responsibilities.

**Data Security:** Information and records (data) are managed consistent with the bank's risk strategy to protect the confidentiality, integrity, and availability of information.

1. Data-at-rest classified as critical or confidential is protected through strong encryption.
2. Data-in-transit classified as critical or confidential is protected through strong encryption.
3. Assets are formally managed throughout removal, transfers, and disposition
4. Adequate capacity to ensure availability is maintained.
5. Protections against data leaks are implemented.
6. Integrity checking mechanisms are used to verify software, firmware, and information integrity.
7. The development and testing environment(s) are separate from the production environment.
8. Integrity checking mechanisms are used to verify hardware integrity.

**Information Protection Processes and Procedures:** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational units), processes, and procedures are maintained and used to manage protection of information systems and assets.

1. A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
  2. A System Development Life Cycle to manage systems is implemented
  3. Configuration change control processes are in place.
  4. Backups of information are conducted, maintained, and tested.
  5. Policy and regulations regarding the physical operating environment for bank's assets are met.
  6. Data is destroyed according to policy.
  7. Protection processes are improved.
  8. Effectiveness of protection technologies is shared.
  9. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
  10. Response and recovery plans are tested.
  11. Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
  12. A vulnerability management plan is developed and implemented.
-



**Maintenance:** Maintenance and repairs of information system components are performed consistent with policies and procedures.

1. Maintenance and repair of bank's assets are performed and logged, with approved and controlled tools.
2. Remote maintenance of bank's assets is approved, logged, and performed in a manner that prevents unauthorized access.

**Protective Technology:** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
2. Removable media is protected and its use restricted according to policy.
3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
4. Communications and control networks are protected.
5. Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

## DETECT

**Anomalies and Events:** Anomalous activity is detected and the potential impact of events is understood.

1. A baseline of network operations and expected data flows for users and systems is established and managed.
2. Detected events are analyzed to understand attack targets and methods.
3. Event data are collected and correlated from multiple sources and sensors
4. Impact of events is determined.
5. Incident alert thresholds are established.

**Security Continuous Monitoring:** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

1. The network is monitored to detect potential cybersecurity events.
  2. The physical environment is monitored to detect potential cybersecurity events
  3. Personnel activity is monitored to detect potential cybersecurity events.
  4. Malicious code is detected.
  5. Unauthorized mobile code is detected.
  6. External service provider activity is monitored to detect potential cybersecurity events.
  7. Monitoring for unauthorized personnel, connections, devices, and software is performed.
  8. Vulnerability scans are performed at least quarterly.
-



**Detection Processes:** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

1. Roles and responsibilities for detection are well defined to ensure accountability.
2. Detection activities comply with all applicable requirements.
3. Detection processes are tested.
4. Event detection information is communicated.
5. Detection processes are continuously improved.

## RESPOND

**Response Planning:** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. Response plan is executed during or after an incident.

**Communications:** Response activities are coordinated with internal and external stakeholders.

1. Personnel know their roles and order of operations when a response is needed.
2. Incidents are reported consistent with established criteria.
3. Information is shared consistent with response plans.
4. Coordination with internal and external stakeholders occurs consistent with response plans.
5. Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
6. Incident response exercises and scenarios across departments are conducted at least annually.

**Analysis:** Analysis is conducted to ensure effective response and support recovery activities.

1. Notifications from detection systems are investigated.
2. The impact of the incident is understood.
3. Forensics are performed.
4. Incidents are categorized consistent with response plans.
5. Processes are established to receive, analyze and respond to vulnerabilities disclosed to the bank from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

**Mitigation:** Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

1. Incidents are contained.
  2. Incidents are mitigated.
  3. Newly identified vulnerabilities are mitigated or documented as accepted risks.
-



**Improvements:** The response activities are improved by incorporating lessons learned from current and previous detection/response activities.

1. Response plans incorporate lessons learned.
2. Response strategies are updated.

## **RECOVER**

**Recovery Planning:** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. Recovery plan is executed during or after a cybersecurity incident.

**Improvements:** Recovery planning and processes are improved by incorporating lessons learned into future activities.

1. Recovery plans incorporate lessons learned.
2. Recovery strategies are updated.

**Communications:** Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

1. Public relations are managed.
2. Reputation is repaired after an incident.
3. Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

CONSULTATION