Cybersecurity Framework

Version 1.0 (2026)

Bangladesh Bank

The page is intentionally left blank

Technical Committee

Chairman

Mr. Debdulal Roy
Executive Director (ICT)
Bangladesh Bank

Members

Mr. Md. Amir Hossain Pathan
Chief Information Security Officer (CISO)
Cyber Security Unit (CSU)

Mr. Mohammad Masud Anwar
Additional Director (ICT)
Information and Communication Technology Department, Bangladesh Bank

Mr. Jayanta Kumar Bhowmick
Additional Director (ICT)
Payment System Department-2, Bangladesh Bank

Ms. Latifa Khanam
Additional Director
Banking Regulation and Policy Department-1, Bangladesh Bank

Mr. S. M. Tofayel Ahmad
Additional Director (ICT)
Information and Communication Technology Department, Bangladesh Bank
and Member Secretary

Mr. Md. Kaderuzzaman
Additional Director (Ex-Cadre Law)
Law Department, Bangladesh Bank

Mr. Prakash Chandra Mondal
Joint Director (ICT)
Information and Communication Technology Department, Bangladesh Bank

Mr. Fahad Zaman Chowdhury
Joint Director (ICT), Bangladesh Bank

Mr. Hafiz Al Asad
Assistant Chief Information Security Officer
Cyber Security Unit, Bangladesh Bank

Dr. Nurullah Shahin
Joint Director (ICT)
Enterprise Risk Management Department, Bangladesh Bank

Mr. Enamul Mowla
Chief Information Technology Officer
Agrani Bank PLC

Mr. S. M. Mizanur Rahman
Senior Vice President and CISO
Islami Bank Bangladesh PLC

Mr. Md. Abul Kalam Azad
Senior Vice President and CISO
Eastern Bank PLC

Mr. Md Sayed Bin Sodrul
Director, Country Technology and Cyber Risk Officer
Standard Chartered Bank

Mr. Khandakar Rafiqual Islam
Senior Vice President and Head of Operational Risk
Prime Bank PLC.

In addition, the following officials have also contributed to the preparation of this framework:

Mr. Muhammad Zakir Hasan
Executive Director (ICT)
Bangladesh Bank

Mr. Mohammad Imtiaz Kabir
Deputy Chief Information Security Officer
Cyber Security Unit, Bangladesh Bank

Mr. Md. Imran Khan
Joint Director (ICT)
Information and Communication Technology Department, Bangladesh Bank

Mr. Md. Golam Mahmud
Joint Director (ICT)
Information and Communication Technology Department, Bangladesh Bank

Mr. Md. Mushfiqur Rahman
Senior Vice President and Chief Information Technology Officer (CITO)
Standard Islami Bank PLC

Table of Contents

List of Abbreviation vii
1 INTRODUCTION 1
1.1 Scope 1
1.2 Objective 2
1.3 Organizational Responsibility 2
1.4 Cyber Risk Management 3
1.5 Framework Basics 3
1.5.1 Framework Core 3
1.5.2 Functions 3
1.5.3 Categories 4
1.6 Disclaimer 6
2 PREPARATION 7
2.1 Introduction 7
2.2 Governance 7
2.3 Management 8
2.4 Coordination of Framework Implementation 9
2.5 Cyber Incident Response Team 10
2.6 Self-Assessing Cybersecurity Risk with the Framework 11
2.7 Policies and Procedures 11
2.8 Processes 12
2.9 Framework 12
2.10 Frameworks Category 12
2.10.1 Component of Control Frameworks 13
2.11 Countermeasures 13
2.12 Awareness and Training 13
3 IDENTIFY 14
3.1 Introduction 14
3.1.1 Asset Management 14
3.1.2 Business Environment 15

3.1.3 Risk Governance 15
3.1.4 Risk Assessment 16
3.1.5 Risk Management Strategy 17
3.1.6 Suppliers Risk Management 17
3.1.7 Cloud Risk Management 17
3.1.8 Insider Threat and Employee Risk Management 18
3.1.9 Recording Logs 19
4 PROTECT 21
4.1 Introduction 21
4.1.1 Identity Management 21
4.1.2 Access Control 21
4.1.3 ICT Infrastructure Security and Procedures 22
4.1.4 Preventing Execution of Unauthorized Software 24
4.1.5 Encryption and Data Security 25
4.1.6 Information Protection Processes and Procedures 27
4.1.7 Maintenance 28
4.1.8 Protective Technology 28
5 DETECT 30
5.1 Introduction 30
5.1.1 Detection of Anomalies and Events 30
5.1.2 Continuous Monitoring of Security 31
5.1.3 Detection Processes and Procedures 33
6 RESPOND 34
6.1 Introduction 34
6.1.1 Response Planning 34
6.1.2 Communications 34
6.1.3 Analysis 35
6.1.4 Mitigation 37
6.1.5 Continuous Improvements 38
7 RECOVERY 39
7.1 Introduction 39

7.1.1 Recovery Planning 39
7.1.2 Continuous Improvement Metrics and KPIs 40
7.1.3 Communications 41
8 Reporting 42
8.1 Introduction 42
8.1.1 Communications 42
8.1.2 Reporting Criteria 43
8.1.3 Cybersecurity Audit 43
8.1.4 Lesson-Learned 44
8.1.5 Post Incident Analysis 45
9 CONCLUSION 46
Appendix A: CYBERSECURITY SOLUTIONS AND TECHNOLOGIES 47
Appendix B: SOLUTION DETAILS 48
Appendix C: SAMPLE CHECKLIST FOR CYBERSECURITY ASSESSMENT 49

The page is intentionally left blank

List of Abbreviation

APT	Advanced Persistent Threat
ATP	Advanced Threat Protection
CHD	Card Holder Data
CASB	Cloud Access Security Broker
CCO	Chief Compliance Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
DLP	Data Loss Prevention
DRM	Digital Rights Management
DDOS	Distributed Denial of Service
DMZ	Demilitarized Zone
EDR	Endpoint Detection and Response
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
ICTRMF	ICT Risk management Framework
IRT	Incident Response Team
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
MITM	Man-in-the-Middle
MSP	Managed Service Provider
MSSP	Managed Security Services Provider
NIST	National Institute of Standards and Technology

OEM	Original Equipment Manufacturer
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
RBAC	Role-Based Access Control
SECaaS	Security as a Service
SIM	Security Information Management
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOAPA	Security Operations and Analytics Platform Architecture
SOAR	Security Orchestration, Automation and Response
SAD	Sensitive Authentication Data
UEBA	User and Entity Behavior Analysis
UBA	User Behavior Analytics

1 INTRODUCTION

Banks and financial institutions have been changing through rapid digital transformation. It is noteworthy that digitalization in the financial sector significantly improved the financial services to the customers. However, the gradual expansions of ICT-based financial services inadvertently brought cyber threats, broaden cyber-attack surfaces, and increase vulnerabilities. Consequently, cyber resilience becomes a key issue to act as a safeguard of financial systems.

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. A strong Cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort the information systems and sensitive data. It aims to reduce the risk of cyber-attacks and protect systems, networks, data and technologies from vulnerability exposure and potential threats. Everyone who is connected to the Internet needs Cybersecurity. This is because most cyber attacks are automated and aim to exploit common vulnerabilities rather than specific websites or organizations.

As a regulator, Bangladesh Bank introduces Cybersecurity Framework for banks and other financial institutions that are under its regulation. The purpose of this framework is to ensure Cybersecurity governance and build better resilience against cyber threats. The framework is developed based on six core functions mentioned in the NIST Cybersecurity Framework i.e., Govern, Identify, Protect, Detect, Respond and Recover. The controls of the framework are mostly based on ISO 27001, national ICT Security Policies, ICT Security Guidelines of Bangladesh Bank and other international standards. It is noted that the framework will act as baseline for Cybersecurity standards and controls that are designed to fulfill the minimum requirements for safeguarding against cyber threats.

1.1 Scope

This framework is applicable to Banks, Financial Institutions, Mobile Financial Service Providers (MFSP), Payment Service Providers (PSP), Payment System Operators (PSO) and other financial/payment service providing organizations. Throughout this framework all these entities will be termed together as "**The Organization".**

This framework addresses the approaches and principles necessary for adoption of Cybersecurity measures by the Organization. However, this framework does not prescribe or recommend any specific Cybersecurity service, service arrangement, service agreement, service provider or deployment models. The Organization must perform their own analysis to determine if Cybersecurity Framework meets their strategic aims whilst managing any associated risks and compliance with regulatory requirements.

1.2 Objective

The objectives of this framework are to establish a minimum baseline for the management of Cybersecurity in the organization based on the following key areas to:

a) Protect financial stability;
b) Detect and respond to cyber threats;
c) Create a common approach for addressing Cybersecurity;
d) Achieve an appropriate maturity level of Cybersecurity practices;
e) Define roles and responsibilities of relevant parties;
f) Address Cybersecurity practices with due diligence;
g) Ensure security and privacy requirements;
h) Develop and implement robust cyber risk management strategies to minimize vulnerabilities;
i) Develop stakeholders' awareness to protect information in cyber environment;
j) Ensure a secure environment for data processing;
k) Ensure best practices (industry standard) of the usage of technology;
l) Build a Cybersecurity culture;
m) Ensure compliance with relevant laws regulations and industry best practices;

1.3 Organizational Responsibility

Managing security and privacy risks is a complex and multifaceted undertaking that requires:

1. Establishing well-defined security and privacy requirements, along with ongoing oversight, for third-party service providers, contractors, and suppliers who interact with the organization's systems and data;
2. The use of trustworthy information system components based on state-of-the-practice hardware, firmware, and software development and acquisition processes;
3. Rigorous Cybersecurity and privacy planning and system development life cycle management;
4. The application of system security and privacy engineering principles and practices to securely develop and integrate system components into information systems;
5. The employment of security and privacy practices that are properly documented and integrated into and supportive of the institutional and operational processes of organizations;

6. Continuous monitoring of information systems and organizations to determine the ongoing effectiveness of controls, changes in information systems and environments of operation, and the state of organization-wide security and privacy practices;
7. Conducting regular training sessions using internal/external resources to ensure users can recognize and respond to security and privacy threats effectively;
8. Implementing customized training programs tailored to specific job roles, including system administrators, database administrators, network administrators, and developers, to address their unique security and privacy responsibilities.

1.4 Cyber Risk Management

Cyber risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organization can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk appetite.

1.5 Framework Basics

The Framework provides a common language for understanding, managing, and expressing Cybersecurity risk to internal and external stakeholders. It can be used to help identifying and prioritizing actions for reducing Cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage Cybersecurity risk across entire organization or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

1.5.1 Framework Core

The Framework core provides a set of activities to achieve specific Cybersecurity *outcomes*, and guidance to achieve those outcomes. The core is not a checklist of actions to perform. It presents key Cybersecurity outcomes identified by stakeholders as helpful in managing Cybersecurity risk. The core comprises four elements: Functions, Categories, Subcategories, and Informative References.

1.5.2 Functions

The Framework is aligned with the NIST Cybersecurity Framework, incorporating 7 functions, namely-Preparation and Govern, Identify, Protect, Detect, Respond, Recovery, and Reporting. These functions aid an organization in expressing its

management of Cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving through learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in Cybersecurity.

1.5.3 Categories

Categories are the subdivisions of a Function into groups of Cybersecurity outcomes closely tied to programmatic needs and particular activities.

The following table shows the functions and the categories under each function:

Sl. No.	Function	Description	Categories
1.	Preparation and Govern	The organization's Cybersecurity risk management strategy, expectations, Framework, policies and procedures are established, communicated, and monitored.	1) Organizational Context 2) Management 3) Risk Management Strategy 4) Roles, Responsibilities and Authorities 5) Process, Policies and Procedures 6) Framework 7) Oversight 8) Countermeasures 9) Cyber Security Supply Chain Management 10) Awareness and Training

Sl. No.	Function	Description	Categories
2	Identify	Identification of critical assets and management of Cybersecurity risks.	1) Asset Management 2) Business Environment 3) Risk Governance 4) Risk Assessment 5) Risk Management Strategy 6) Suppliers Risk Management 7) Cloud Risk Management 8) Employee Risk Management 9) Recording
3	Protect	Safeguarding continually identified assets by deploying controls such as security architecture mechanisms, event correlation systems, intrusion prevention and detection systems, and enforcement of secure configurations.	1) Containment 2) Identity Management 3) Access Control 4) ICT Infrastructure Security and Procedures 5) Preventing Execution of Unauthorized Software 6) Data Security 7) Training 8) Maintenance 9) Protective Technology
4	Detect	Detecting events or incidents related to attacks or anomalies through continuous monitoring of its infrastructure.	1) Detection of Anomalies and Events 2) Continuous Monitoring of Security 3) Detection Processes and Procedures 4) Evaluation
5	Respond	Take steps to assess the incident impact and take appropriate response measures including escalation to relevant authorities.	1) Eradication 2) Response Planning 3) Escalation 4) Communication 5) Analysis 6) Mitigation 7) Improvement
6	Recover	Recover from incident in a timely manner adequately following the organization's incident management, business continuity and disaster recovery policies and procedures and to ensure that there is no loss of confidential data and that its IT assets are protected against cyber-attacks.	1) Recovery Planning 2) Recover 3) UAT 4) UVT 5) Security and Risk Assessment 6) Go-Live 7) Continuous Improvement

Sl. No.	Function	Description	Categories
7	Reporting	Organization needs cyber incident reporting to keep their workplace safe, accessible, and compliant. Cyber Incident reporting helps organization identify trends, analyze the root cause of a cyber incident, and make necessary adjustments to prevent similar incidents from occurring.	1) Communication 2) Reporting 3) Lesson Learned 4) Post Incident Review

1.6 Disclaimer

This framework is prepared in such a way that it conforms to international standards, national ICT Security Policies and Bangladesh Bank's ICT Security Guidelines. If any of the control(s) or statement(s) of this framework contradict any Act/ Law/ Guidelines/ Policies/ Framework issued by the Government of Bangladesh then that will supersede the control(s) of this framework. However, in case of any contradiction arises with the existing guidelines/circulars issued by Bangladesh Bank then it may be resolved upon request from the Organization.

2 PREPARATION

2.1 Introduction

The key to a successful Cybersecurity management system is to prepare well, ensure timely detection, and respond to incidents. While facing any security incidents, an absolute shield against cyber threats may not exist. Best practice may therefore be, 'just' involve good preparation against different types of Cybersecurity threats. The preparation phase can be broken down into six aspects: **Policies, Procedures, Processes, Framework, Countermeasures, and Training.** It provides directions on how to complete security policies, asset identification, risk assessment, threat protection, instruction detection, event response, disaster recovery, security drills, and others, all of which must be considered in the Cybersecurity mechanism.

2.2 Governance

Organizational Context: Organization should understand circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements- surrounding the organization's Cybersecurity risk management.

Cybersecurity Supply Chain Risk Management: Cybersecurity supply chain risk management processes should be identified, established, managed, monitored, and improved by organizational stakeholders.

Roles, Responsibilities, and Authorities: Cybersecurity roles, responsibilities, and authorities should be established and communicated to foster accountability, performance assessment, and continuous improvement. The following aspects shall be addressed:

a) Enterprise security governance activities involve the development, institutionalization, assessment, and improvement of an organization's Enterprise Risk Management (ERM) and security policies;
b) Governance is a company's strategy for reducing the risk of unauthorized access to information technology systems and data;
c) ICT Security Governance ensures that the ICT security functions and operations are efficiently and effectively managed;
d) Governance of enterprise security includes determining how various business units, personnel, executives, and staff should work together to protect an organization's digital assets, ensure data loss prevention and protect the organization's public reputation.

2.3 Management

In response to the cyber-attacks, management at the organization has to set up a management strategy to protect its IT assets from cyber-attacks and respond to any cyber-attacks, threats in a timely and appropriate manner to ensure confidentiality, integrity and availability of data/IT Systems. The Cybersecurity strategy to be used at the organization is to **Identify, Protect, Detect, Respond, and Recover and Learn** which is as explained below:

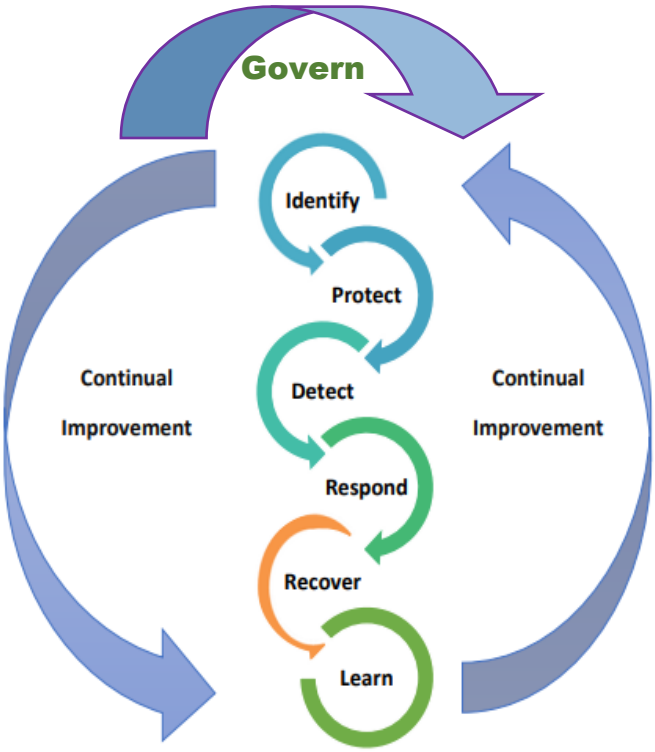

Figure 2.3: The Cybersecurity strategy

a) The top management ensures that appropriate Information security controls and functions are in place;
b) The top management contributes to ICT security planning to ensure that resources i.e. process and technology are allocated consistently with business objectives and to ensure that sufficient and qualified technical staff are employed;
c) ICT Security Management is responsible for the ICT Governance of the Organization that includes but not limited to Roles and Responsibilities, ICT Security Policy, Documentation, Internal and External Information System Audit, Training and Awareness, Insurance or Risk coverage fund;
d) The top management ensures the periodic review of implemented security controls and provides necessary directives as needed to maintain security standards.

2.3.1 Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) plays a crucial role in an organization's Cybersecurity posture and overall risk management.

(a) The organization shall recruit a qualified CISO.
(b) The organization shall approve required human resources for CISO.
(c) The organization shall approve sufficient financial budget for CISO.
(d) A CISO should have industry accepted academic and professional certification.

2.4 Coordination of Framework Implementation

The information and decisions flow levels within an organization can be:

1. Board of Directors
2. Senior Management
3. Business/ Process
4. Implementation/ Operations

The senior management level is responsible for communicating the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/ operations level communicates the profile implementation progress to the business/ process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/ operations level for awareness of business impact.

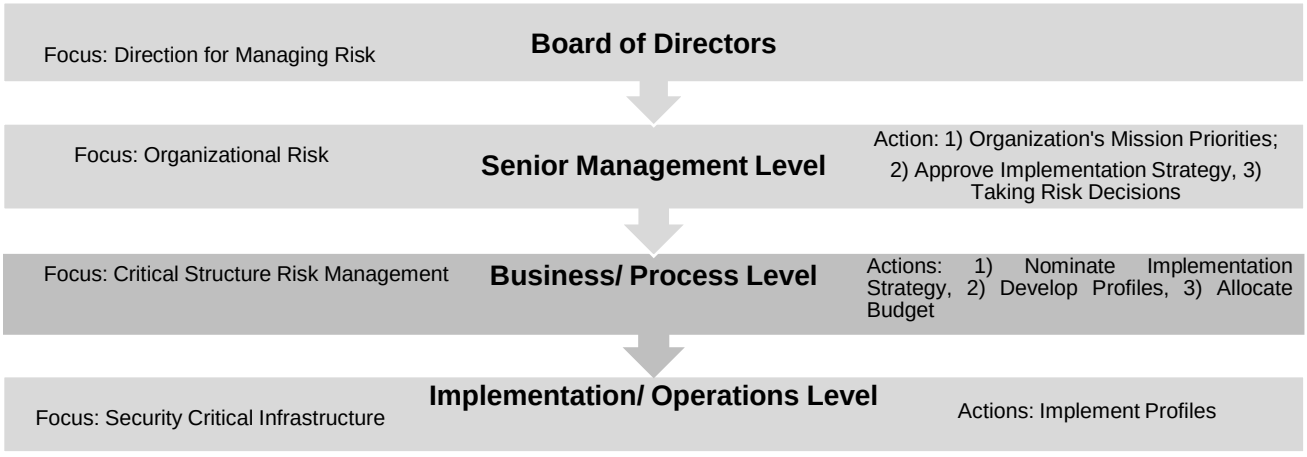

Figure 2.4: Coordination of Framework Implementation

2.5 Cyber Incident Response Team

The Cyber Incident Response Team (CIRT) to be formed to address any incidents and initiate immediate action to resolve the same. The Team defines procedures to proactively address potential threats/ risks arising out of cyber/computer incidents. Such teams are formed ad hoc; and are based on the severity and impact of the incidents. But most incidents are to be handled at the Cyber Incident Response Team Leader level.

The team should consist of the following members:

1. **Cyber Incident Management Leader (CIML):** The Managing Director (MD) or similar designated or delegated person would be the IML and should be responsible for overall management of high-severity incidents. The IML is responsible for taking critical decisions regarding business operations/process changes during/after an incident.

   [*The CIML or a person designated by him only can deal with the media in case of any incidents*.]

2. **Cyber Incident Management Coordinator (CIMC):** The HOICTD/CITO or similar designated or delegated person plays the role of CIMC. CIMC is responsible for coordinating with the other divisional heads to manage and resolve the cyber incident. The CIMC should work with the Cyber Incident Response Team Leader to contain the damage caused by the incident and should be the focal point for recovery efforts.

3. **Cyber Incident Response Team Leader (IRTL): Head of Information Security /** CISO should be the Team Leaders for all Cybersecurity related incidents. They should be part of any cyber incident response team. The CIRTL should be the 'one-point contact' for all the users for all cyber incidents. CIRTL is responsible for evaluating the incident and appropriately initiating the escalation process. CIRTL should delegate action on incidents to Information Security Committee.

4. **Cyber Incident Response Team members (IRTM):** The Supervisors of divisions/units/ departments are the team members for cyber incident response. They should get detailed briefing from CIRTL before acting on any incident. IRTL and IR Team members should have the list of all emergency contact details of the entire Incident Response Team, Vendors, Suppliers, Service providers, etc.
   [*An emergency pocket sized card can be prepared containing contact numbers of the Incident Response team members and distributed to all the employees.*]

2.6 Self-Assessing Cybersecurity Risk with the Framework

The framework for Cybersecurity enables the reduction of risk by improving the management of Cybersecurity risk to organizational objectives. The Framework helps to measure and assign values to the risk by calculating the cost and benefits of steps taken to reduce risk to acceptable levels. The better the measurement of risk, costs, and benefits of Cybersecurity strategies and steps, the more rationality, effect, and value it will add to the Cybersecurity approach and investments. Self-assessment and measurement tactics improve the decision-making process regarding investment priorities. Self-assessment can be accomplished internally or by seeking a third-party assessment. If done properly and with an appreciation of limitations, these measurements can provide a basis for strong trusted relationships, both inside and outside of an organization.

a) Self-assessment makes choices about how different portions of the Cybersecurity operation should influence the selection of Target Implementation Tiers;
b) Self-assessment enables evaluation of the organization's approach to Cybersecurity risk management by determining Current Implementation Tiers;
c) Self-assessment enables prioritizing Cybersecurity outcomes by developing target profiles;
d) By assessing the current profile self-assessment will determine the degree to which specific Cybersecurity steps achieve desired Cybersecurity outcomes;
e) Measuring the degree of implementation for controls catalogs or technical guidance listed as informative references.

2.7 Policies and Procedures

The organization shall develop policies and procedures to:

a) Provide guidance, consistency, accountability, efficiency, and clarity on how an organization operates in case of Cybersecurity;
b) Identify key activities;
c) Provide guidance for the board on how to handle issues as they arise;
d) Provide a roadmap for day-to-day operations. They ensure compliance with laws and regulations, give guidance for decision-making, and streamline internal processes;
e) Ensure that the organization is operating in a way that is consistent with its values and goals;
f) Ensure the organization's processes do not deviate or deteriorate over time, even if key board members, contractors, or employees leave;

g) Improve overall organizational performance by keeping everyone “on the same page” when it comes to expectations and issues;
h) Maintain consistency and control over organizational operations;
i) Keep the company running smoothly and efficiently;
j) Help employees know what is expected of them and what they should do in certain situations;
k) Provide guidance for developing Cybersecurity hygiene within the organization by ensuring adherence to regulatory requirements, standards, and best practices.

2.8 Processes

Cybersecurity processes are the requirements and steps that Cybersecurity analysts implement as they execute their duties. The organization shall develop processes to:

a) Implement an effective Cybersecurity strategy;
b) Define how an organization's activities, roles, and documentation are used to mitigate information risks;
c) Design and deploy the process to protect sensitive business information from modification, disruption, destruction, and inspection.

2.9 Framework

Cybersecurity frameworks are sets of documents describing guidelines, standards, and best practices designed for Cybersecurity risk management. Cybersecurity frameworks:

a) Offer guidance, helping information security leaders manage their organization's cyber risks more intelligently;
b) Help teams to address Cybersecurity challenges, providing a strategic, well-thought plan to protect organizational data, infrastructure, and information systems;
c) Enable long-term Cybersecurity and risk management;
d) Ripple effects across supply chains and vendor lists;
e) Bridge the gap between technical and business-side stakeholders;
f) Built for future regulation and compliance requirements.

2.10 Frameworks Category

Frameworks break down into categories such as Control Framework, Program Framework and Risk Framework. This framework is based on control framework only.

2.10.1 Component of Control Frameworks

a) Develops a basic strategy for the organization's Cybersecurity Department/Division;
b) Provides a baseline group of security controls;
c) Assesses the present state of the infrastructure and technology;
d) Prioritizes implementation of security controls.

2.11 Countermeasures

a) A countermeasure is an action, device, procedure, or technique that reduces a threat, vulnerability, or attack by eliminating or preventing it, minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken;
b) A safeguard or countermeasure prescribed for an information system or an organization is designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements;
c) Countermeasures are devices, signals, and techniques deployed to impair or eliminate the operational effectiveness of an attack by an enemy force.

2.12 Awareness and Training

The organization shall arrange awareness and training programs to achieve objectives of the following areas:

a) Cybersecurity awareness education to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements;
b) Periodic training to all staffs on the organization's security policies and cyber-security hygiene practice with explanations as to why the policies are important and compliance;
c) Training facilities and standard certifications, i.e., CEH, CFR, CISA, ISMS, CISSP, CISM, CRISC, CPTE, CPEH, SCNP, SSCP, CCSP, NSCP, AIS, CPTS, CCFT, CompTIA, OSCP, Cloud Computing, Emerging Technologies etc., for the information security division/department/unit staffs to ensure the development of expert Cybersecurity specialists;
d) Training for privileged users, senior executives, and physical security personnel, information security personnel to understand their roles and responsibilities;
e) Awareness or training for third-party/vendors so that the third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities etc.

3 IDENTIFY

3.1 Introduction

Develop an organizational 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 Framework. Understanding the business context, the resources that support critical functions, and the related Cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

3.1.1 Asset Management

3.1.1.1 The Organization shall draw and maintain an inventory of all assets associated with information and information processing facilities which should be reviewed and updated within a regular interval. The inventory shall include:

a. Model of device;
b. Location of device (for example, the address of the site or facility where the device is located);
c. Device serial number or another method of unique identification;
d. Asset classification;
e. Purpose of the asset/service name.

3.1.1.2 The Organization shall establish the classification of assets. The Organization shall classify data/information based on information classification/ sensitivity criteria of the organization's ICT Risk Management Framework (ICTRMF);

3.1.1.3 Physical devices and systems within the Organization's information and information processing facilities shall be inventoried, identified, and labeled;

3.1.1.4 The inventory shall include business data, customer data, business applications, supporting IT infrastructure, and facilities (hardware/software/ network devices, key personnel, services, etc.);

3.1.1.5 The Organization shall inventory software platforms and applications within the Organization;

3.1.1.6 The Organization shall catalog external information systems;

3.1.1.7 The Organization shall prioritize resources (e.g., hardware, devices, data, and software) based on their classification, criticality, and business value;

3.1.1.8 Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) shall be established;

3.1.1.9 Reviewing and updating of the ICT asset inventory need to be done regularly;

3.1.1.10 The Organization shall protect the assets adequately from unauthorized access, misuse, or fraudulent modification, insertion, deletion, substitution, suppression, or disclosure;

3.1.1.11 The Organization shall establish rules for the acceptable use of information and assets associated with information and information processing facilities.

3.1.2 Business Environment

3.1.2.1 The Organization shall understand and prioritize its mission, objectives, stakeholders, and activities. This information shall use to establish Cybersecurity roles, responsibilities, and risk management decisions;

3.1.2.2 The Organization shall identify and communicate its role in the supply chain;

3.1.2.3 The Organization shall identify its critical infrastructure and communicate to relevant stakeholder;

3.1.2.4 The Organization shall identify dependencies and critical functions for the delivery of critical services;

3.1.2.5 The Organization shall establish resilience requirements to support the delivery of critical services.

3.1.3 Risk Governance

3.1.3.1 The Organization shall establish policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements for the management of Cybersecurity risk;

3.1.3.2 The Organization shall publish, and communicate the policies, procedures, and processes for Cybersecurity to employees and relevant external parties;

3.1.3.3 The Organization shall clearly define and allocate the roles and responsibilities of each of the three lines of defense (Management control for business and IT functions, Information and Technology Risk Management functions, and Internal Audit) within the Cybersecurity policy;

3.1.3.4 The Organization shall coordinate and align information security roles and responsibilities with internal roles and external partners;

3.1.3.5 The Organization shall establish Cybersecurity roles and responsibilities for the third-party stakeholders (suppliers, customers, partners, OEM, etc.);

3.1.3.6 The Organization shall understand and manage legal and regulatory requirements regarding Cybersecurity, including privacy and civil liberties obligations;

3.1.3.7 The Organization shall address Cybersecurity risks in Governance and risk management processes;

3.1.3.8 The Organization shall establish the priorities for mission-critical services and their dependencies on critical services.

3.1.4 Risk Assessment

3.1.4.1 The Organization shall understand the Cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals;

3.1.4.2 The Organization shall identify and document asset vulnerabilities. Threat and vulnerability information is received from information-sharing forums and sources;

3.1.4.3 The Organization shall identify and document threats, both internal and external. Potential business impacts and likelihoods shall be identified;

3.1.4.4 The Organization shall conduct regular and comprehensive cyber risk assessments that consider people (i.e. employees, customers, and other external parties), processes, data, and technology across all its business activities;

3.1.4.5 The Organization shall conduct configuration assessments periodically for hardware and software/applications;

3.1.4.6 The Organization shall determine risk score using threats, vulnerabilities, likelihoods, impacts, etc. parameters following the ICT Risk Management Framework (ICTRMF);

3.1.4.7 The Organization shall identify and define the priority of risk responses;

3.1.4.8 The Organization shall collect feeds for the cyber threat intelligence from various information-sharing forums and sources;

3.1.4.9 The Organization shall conduct configuration assessments periodically for hardware and software/applications, Network, Cloud Platform/Service etc.;

3.1.4.10 In case of successful Risk Completion, the organization needs to define the risk responsibilities to individuals. The risk accountability applies to those who own the required resources and have the authority to approve the execution and/or accept the outcome of activity within specific cyber risk processes. Ownership of risk stays with the owner or custodian whoever is in a better position to mitigate the identified risk for that specific information and information processing asset;

3.1.4.11 The Organization shall review and approve risk appetite and tolerance change on a regular basis, especially for new technology, new organizational structure, new business strategy, and other factors that require the enterprise to reassess its risk portfolio.

3.1.5 Risk Management Strategy

The Organization shall ensure priorities, constraints, risk tolerances, and assumptions which are established and used to support operational risk decisions:

3.1.5.1 The Organization shall establish the ICT Risk management processes;

3.1.5.2 The Organization shall determine and clearly express the risk tolerance. Determination of risk tolerance shall be identified from its role in critical infrastructure and sector-specific risk analysis;

3.1.5.3 An information security risk management personnel shall need to understand how information security-related failures or events can impact enterprise objectives and cause direct or indirect loss to the enterprise;

3.1.5.4 A business person has to understand how ICT-related failures or events can affect key services and processes.

3.1.6 Suppliers Risk Management

The Organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The Organization needs to establish the processes to identify, assess and manage supply chain risks.

3.1.6.1 The Organization shall prepare cyber supply chain risk management processes that are identified, established, assessed, managed, and agreed to by organizational stakeholders;

3.1.6.2 The Organization shall contract with suppliers and third-party partners to implement appropriate measures to meet the objectives of the organization's Cybersecurity program;

3.1.6.3 The Organization shall routinely assess the suppliers and third-party partners using audits, test results, or other forms of evaluations to confirm that they are meeting their contractual obligations;

3.1.6.4 The Organization shall conduct response and recovery planning and testing with suppliers and third-party providers.

3.1.7 Cloud Risk Management

3.1.7.1 There shall be a clear strategy for using cloud computing services consistent and aligned with the organization's overall IT strategy, architecture, risk appetite, level of governance, management comfort and ability to monitor the cloud service provider;

3.1.7.2 The Organizational cloud strategy shall be aligned with long-term business objectives;

3.1.7.3 The Organization's cloud-hosted infrastructure shall be scalable, resilient, and shall have appropriate security controls in place;

3.1.7.4 The Organization's cloud services shall meet regulatory and compliance requirements;

3.1.7.5 The contractual obligations of cloud providers shall be robust and clearly aligned with your business expectations;

3.1.7.6 The Organization shall be aware of all cloud services being used across the organization;

3.1.7.7 The Organization shall perform the audit on its third-party cloud provider;

3.1.7.8 There shall be SLA between the Organization and the cloud provider regarding ensuring the data security of the Organization;

3.1.7.9 The Organization shall follow all the controls of the **'Guideline on Cloud Computing'** formulated by Bangladesh Bank and follow the country's laws and regulations.

3.1.8 Insider Threat and Employee Risk Management

3.1.8.1 The Organization shall ensure the trustworthiness of staff by performing staff screening periodically;

3.1.8.2 The Organization shall perform continuous behavioral monitoring of their employees;

3.1.8.3 The Organization shall organize a catch-up process as part of the periodic screening (sometimes also referred to as re-screening);

3.1.8.4 The screening process for initial employment includes the following verifications:

a. Identity verification;
b. Confirmation of full details of qualifications;
c. Confirmation of previous employment history;
d. Details of any past or pending civil or criminal proceedings against the employee;
e. Validation of any involvement in external businesses that could result in a conflict of interest;
f. Financial credit verification.

3.1.8.5 The periodic screening process includes the following verifications:

a. Details of any pending civil or criminal proceedings against the employee;
b. Validation of any involvement in external businesses that could result in a conflict of interest;
c. Financial credit verification.

3.1.9 Recording Logs

The ICT function has to ensure that critical user activities, exceptions, and security events log are enabled and stored to assist in future investigations and access control monitoring for the following areas:

3.1.9.1 User activities, exceptions, and security events have to be logged and monitored;

3.1.9.2 The activities of users with high levels of access (privileged users such as system administrators and system operators) have to be logged and independently reviewed on a regular basis;

3.1.9.3 The Organization can use Privileged Access Management (PAM) system to identify and authorize privileged account users across the Organization;

3.1.9.4 All access to critical applications and networks have to be monitored for suspicious activities or security breaches. Adequate response mechanisms have to be in place for containing security breaches;

3.1.9.5 The audit logs have to be retained based on the record retention requirements;

3.1.9.6 The clocks of all relevant information processing systems within the Organization have to be synchronized with an agreed accurate time source;

3.1.9.7 The utilization of information systems has to be monitored to ensure their continued and reliable operation;

3.1.9.8 The Organization may use Identity Access Management (IAM) system to identify, authenticate and authorize users, devices, applications, databases, workloads, etc.;

3.1.9.9 Activity and audit logs have to be generated, monitored, and retained for the following:

a. Authorized access;
b. Privileged operations;
c. Unauthorized access attempts;
d. Changes to, or attempts to change, system security settings and controls;
e. Event timestamp and access to the system at an unauthorized time frame;
f. Actor or service that created, edited, or deleted the event (user ID or API ID);
g. Application, device, system, or object that was impacted (IP address, device ID, etc.);
h. Source from where the actor or service originated (country, hostname, IP address, device ID, etc.);
i. Custom tags specified by the user, such as the severity level of the event.

3.1.9.10 The results of the monitoring activities have to be reviewed at specified intervals. The intervals have to be decided as per the criticality of the information systems;

3.1.9.11 Logging facilities and log information have to be protected against unauthorized access, alterations, tempering, and operational problems. Access to logs has to be provided on a ‘need-to-know’ and ‘need-to-have’ basis;

3.1.9.12 The fault logs, security logs, access logs, activity logs, and audit logs of critical applications have to be enabled at all times and protected from unauthorized access, modification, or destruction;

3.1.9.13 Appropriate controls have to be implemented to prevent:

a. Alterations of the message types that are recorded;
b. Alterations or deletions of the log files;
c. Exceeding the storage capacity of the logging media.

3.1.9.14 Information systems have to be configured in a way that administrative access and/or attempts to access are logged. The access to the log files has to be restricted with only the device admin having access to the same;

3.1.9.15 It has to be ensured that the system administrators are restricted to erase or de-activate logs of their own activities.

4 PROTECT

4.1 Introduction

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 event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

4.1.1 Identity Management

4.1.1.1 The Organization shall implement formal user registration and de-registration process to enable the assignment of access rights;

4.1.1.2 The Organization shall implement a formal user access provisioning process to assign or revoke access rights for all user types of all systems and services by the access control policy;

4.1.1.3 The Organization shall implement a centralized network Authentication, Authorization, and Accounting (AAA) mechanism;

4.1.1.4 The Organization shall restrict and control the allocation and use of privileged access rights. The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract/agreement, or adjusted upon change;

4.1.1.5 The Organization shall check the background verification of all candidates for employment based on the classification of the information to be accessed and the perceived risks;

4.1.1.6 The Organization shall ensure the privacy and protection of Personally Identifiable Information (PII) as required in relevant legislation and regulation where applicable.

4.1.2 Access Control

4.1.2.1 The Organization shall establish, document, and review an access control policy based on business and information security requirements;

4.1.2.2 Access to information and application system functions has to be restricted in accordance with the access control policy;

4.1.2.3 Access to physical and logical assets and associated facilities shall be limited to authorized users, processes, or devices, and to authorized activities and transactions;

4.1.2.4 The Organization shall manage identities and credentials for authorized devices and users;

4.1.2.5 The Organization shall ensure access permissions are managed properly, incorporating the principles of least privilege and separation of duties;

4.1.2.6 The Organization shall manage and protect physical and logical access to assets;

4.1.2.7 Before being granted logical access, users have to complete a “User Access Permission Application Form” that defines access privileges;

4.1.2.8 The access rights of all employees and external party users to information and information processing facilities have to be removed upon termination of their employment, contract, or agreement, or adjusted upon change;

4.1.2.9 The Organization shall closely monitor non-employees (contractual, outsourced, or vendor staff) for access restrictions;

4.1.2.10 User access privileges have to be kept updated for job status changes;

4.1.2.11 The Organization shall securely manage remote access;

4.1.2.12 The Organization shall secure all individual non-console administrative access and all remote access to the data environment using multi-factor authentication;

4.1.2.13 User access shall be locked after a certain amount of unsuccessful login attempts;

4.1.2.14 The Organization shall protect network integrity and incorporate network segregation where appropriate;

4.1.2.15 The Organization shall implement password management systems that shall be secure, and interactive and shall ensure strong passwords;

4.1.2.16 The Organization shall perform regular reviews of user access privileges to verify that privileges are granted appropriately.

4.1.3 ICT Infrastructure Security and Procedures

4.1.3.1 The Organization shall implement security control and procedures with the consideration of the existing organization’s information and communication technology infrastructure to maintain a high level of protection from Cybersecurity threats;

4.1.3.2 The Organization shall manage and control the networks to protect the information in systems and applications;

4.1.3.3 The Organization shall have a detailed design document for network communication which has to be approved by the senior management;

4.1.3.4 The Organization shall identify all network services' security mechanisms, service levels, and management requirements and include in-network services agreements, whether these services are provided in-house or outsourced;

4.1.3.5 The Organization shall establish baseline standards to ensure security for network equipment and conduct regular enforcement checks to ensure that

the baseline standards are applied uniformly and non-compliances are detected and raised for investigation;

4.1.3.6 The Organization shall implement the policy and support security to protect information accessed, processed, or stored at teleworking sites and to manage the risks introduced by using mobile devices;

4.1.3.7 The Organization shall ensure the physical security of all network equipment;

4.1.3.8 The Organization shall manage and control the networks to protect the information in systems and applications. Users shall only be provided access to the network and network services that they have been specifically authorized to use;

4.1.3.9 The Organization shall define and use the required security perimeters to protect areas that contain both sensitive or critical information and information processing facilities. Groups of information services, users, and information systems shall be segregated on networks;

4.1.3.10 The Organization shall protect the information involved in transactions to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay;

4.1.3.11 Telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage;

4.1.3.12 Unauthorized access and electronic tampering have to be controlled strictly. The mechanism has to be in place to encrypt and decrypt sensitive data traveling through WAN or public network;

4.1.3.13 Secure Login feature (i.e. SSH) has to be enabled in network devices for remote administration purposes. Any unencrypted login option (i.e. TELNET) has to be disabled;

4.1.3.14 The Organization shall backup and review rules on network security devices on a regular basis to determine that such rules are appropriate and relevant;

4.1.3.15 Role-based and/or Time-based Access Control Lists (ACLs) have to be implemented in the routers to control network traffic;

4.1.3.16 Real-time health monitoring system for infrastructure management may be implemented for surveillance of all network equipment and servers;

4.1.3.17 The Organization shall be able to automatically detect and block unauthorized network access (e.g., wired, wireless, and remote access);

4.1.3.18 The Organization shall rapidly isolate, restrict or shut down compromised devices from the network;

4.1.3.19 The Organization shall implement DNS protection;

4.1.3.20 The Organization shall implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) for E-mail security;

4.1.3.21 The Organization shall review the following at least daily:

a. All security events;
b. Logs of all system components that store, process, or transmit CHD and/or SAD;
c. Logs of all critical system components;
d. Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

4.1.3.22 The Organization shall implement physical and/or logical controls to restrict access to publicly accessible network ports. For example, network ports located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized;

4.1.3.23 The Organization shall ensure that visitors are escorted at all times in areas with active network ports;

4.1.3.24 Mass storage Read/write access through USB port shall be disabled for end user devices (Laptop/Desktop). It might be enabled for limited duration based on appropriate justification and management approval.

4.1.4 Preventing Execution of Unauthorized Software

4.1.4.1 The Organization shall maintain an up-to-date and centralized inventory of authorized/unauthorized software(s). Whitelisting of authorized applications shall be done;

4.1.4.2 All the software procured and installed by the Organization shall have legal licenses and a record of the same has to be maintained by the respective unit/department;

4.1.4.3 The Organization shall have a mechanism for controlled installation of softwares/applications at end-user devices such as PCs, laptops, workstations, servers, mobile devices, etc.;

4.1.4.4 The Organization shall restrict the accessibility to program source code;

4.1.4.5 The Organization shall have an approved software list with vendor information (outsourcing and in-house). In the case of outsourced software, the organization shall supervise and monitor the activity of outsourced system development;

4.1.4.6 Process flow shall be developed for software development and deployment;

4.1.4.7 There shall be a separate test environment maintained to perform end-to-end testing of the software functionalities before implementation;

4.1.4.8 Any bugs and/or defects found due to design flaws shall be escalated to higher levels;

4.1.4.9 Support agreement has to be maintained with the provider for the application software used in production with the confidentiality agreement;

4.1.4.10 There shall be a real-time backup process in-place for all critical and core applications;

4.1.4.11 The Organization has to establish and appropriately protect secure development environments for system development and integration efforts which cover the entire system development lifecycle;

4.1.4.12 The Organization has to ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. The critical security patches shall be installed within one month of release.

4.1.5 Encryption and Data Security

4.1.5.1 Information and transactional records shall be managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information;

4.1.5.2 The Organization shall appropriately protect Data-at-rest and Data-in-transit taking into consideration the level of risk;

4.1.5.3 The Organization shall perform data classification of all the identified data containing organization-related information with the help of data owners;

4.1.5.4 The data should be classified on the basis of the impact that, the loss of data or the impact of a security breach would have on the business of the organization;

4.1.5.5 The data classification scheme should include:

a. The type of data
b. The criticality of the data
c. The data value

4.1.5.6 The data classification can be:

a. Public
b. Internal
c. Confidential
d. Restricted

4.1.5.7 The information shall be consistently protected throughout its life cycle, from its origination to its destruction;

4.1.5.8 Information shall be protected in a manner commensurate with its sensitivity, no matter where it resides, what form it takes, what technology was used to handle it, and what purpose it serves;

4.1.5.9 The Organization shall maintain adequate capacity to ensure the availability;

4.1.5.10 Data leak protections mechanism shall be implemented;

4.1.5.11 The Organization shall use Integrity checking mechanisms to verify software, firmware, and information integrity;

4.1.5.12 The development and testing environment(s) shall be separated from the production environment;

4.1.5.13 The Organization shall develop and implement the policy on the use of cryptographic controls for the protection of information;

4.1.5.14 Confidential or sensitive information that is stored in laptops/Desktops shall be encrypted;

4.1.5.15 Keep data storage to a minimum by implementing data retention and disposal policies, procedures, and processes that include at least the following for all data storage:

a. Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements;
b. Specific retention requirements for data;
c. Processes for secure deletion of data when no longer needed;
d. A quarterly process for identifying and securely deleting stored sensitive data that exceeds defined retention.

4.1.5.16 Information involved in electronic messaging shall be appropriately protected;

4.1.5.17 The Organization shall ensure that all of its sensitive data are encrypted;

4.1.5.18 The Organization shall ensure that cryptographic keys are securely generated. All materials used in the generation process shall be destroyed after usage and ensure that no single individual knows any key in its entirety or has access to all the constituents making up these keys;

4.1.5.19 Use strong cryptography and security protocols to safeguard sensitive data during transmission over open, public networks, including the following:

a. Only trusted keys and certificates are accepted;
b. The protocol in use only supports secure versions or configurations;
c. The encryption strength is appropriate for the encryption methodology in use.

4.1.5.20 Key data management aspects relevant to data protection:

a. Data availability—ensuring users can access and use the data required to perform business even when this data is lost or damaged;
b. Data lifecycle management—involves automating the transmission of critical data to offline and online storage;
c. Information lifecycle management—involves the valuation, cataloging, and protection of information assets from various sources, including

facility outages and disruptions, application and user errors, machine failure, and malware and virus attacks.

4.1.5.21 The Organization shall assign a dedicated backup administrator or backup responsibility should be owned by a team or person to ensure backup;

4.1.5.22 The Organization shall ensure proper backup in place;

4.1.5.23 The Organization shall implement end-to-end encryption (E2EE) for sensitive data, both at rest and in transit;

4.1.5.24 The Organization shall maintain a 3-2-1 data backup rule: keeping three copies of the data on two storage media, one of which is off-premises;

4.1.5.25 The Organization shall ensure data leak/loss prevention (DLP) solutions are in place to monitor and control data exfiltration.

4.1.6 Information Protection Processes and Procedures

4.1.6.1 The Organization shall develop security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures to maintain and use to manage the protection of information systems and assets;

4.1.6.2 The Organization shall establish and maintain a baseline configuration of information technology/industrial control systems;

4.1.6.3 The Organization shall implement information processing facilities with redundancy that would be sufficient to meet availability requirements;

4.1.6.4 The Organization shall have contractual agreements with employees and contractors stating their and the organization’s responsibilities for information security;

4.1.6.5 The Organization shall control changes to the business processes, information processing facilities, and systems that affect information security;

4.1.6.6 The Organization shall review and test if operating platforms are changed to ensure there is no adverse impact on organizational operations or security;

4.1.6.7 The Organization shall establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation, e.g. during a crisis or disaster;

4.1.6.8 The Organization shall implement a System Development Life Cycle to manage systems;

4.1.6.9 The Organization shall develop configuration change control processes;

4.1.6.10 The Organization shall develop backup procedure which are conducted, maintained, and tested periodically;

4.1.6.11 The Organization shall meet policies and regulations regarding the physical operating environment for organizational assets;

4.1.6.12 Data declassification, archiving, and destruction shall maintain according to policy;

4.1.6.13 The Organization shall continuously improve protection processes;

4.1.6.14 The Organization shall test and share the effectiveness of protection technologies, response and recovery plans with the appropriate parties;

4.1.6.15 The Organization shall incorporate cybersecurity practices into HR processes (e.g., deprovisioning, personnel screening);

4.1.6.16 The Organization shall develop and implement vulnerability management plan.

4.1.7 Maintenance

4.1.7.1 The Organization shall perform maintenance and repair of information system components consistent with policies and procedures;

4.1.7.2 The Organization shall ensure log maintenance and repairmen of organizational assets in a timely manner, with approved and controlled tools;

4.1.7.3 The Organization shall approve, log, and perform remote maintenance of organizational assets in a manner that prevents unauthorized access.

4.1.8 Protective Technology

4.1.8.1 The Organization shall manage technical security solutions to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements;

4.1.8.2 The Organization shall determine, document, implement, and review audit/log records in accordance with the policy;

4.1.8.3 The Organization shall protect removable media and restrict its use according to policy;

4.1.8.4 The Organization shall control access to systems and assets, incorporating the principle of least functionality;

4.1.8.5 The Organization shall ensure communications and control networks are protected;

4.1.8.6 The Organization shall establish baseline standards to ensure security for Operating Systems, Networks, Databases, Applications and portable devices which have to meet the organization’s policy;

4.1.8.7 The Organization shall establish and ensure that the patch management procedures include identification, categorization, and prioritization of security patches. To implement security patches in a timely manner, organization can establish the implementation timeframe for each category of security patches;

4.1.8.8 The Organization shall perform rigorous testing of security patches before deployment into the production environment;

4.1.8.9 The Organization shall ensure 24/7 monitoring for the data center and Disaster Recovery Site (DRS);

4.1.8.10 The Organization shall use a standard secure configuration policy/procedure for all hardware and software assets;

4.1.8.11 The Organization shall restrict the use of unauthorized/ unregistered software and hardware;

4.1.8.12 The Organization shall conduct VAs regularly to detect security vulnerabilities in the ICT environment. The Organization shall deploy a combination of automated tools and manual techniques to perform a comprehensive VA. For web-based systems, the scope of VA has to include common web vulnerabilities such as SQL injection, cross-site scripting, etc.;

4.1.8.13 The Organization shall carry out penetration tests and compromise assessment in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system;

4.1.8.14 All applications and systems that require connections to the Internet or third-party and public networks need to undergo a formal risk analysis during development and before production and all required security mechanisms need to be implemented.

5 DETECT

5.1 Introduction

In case of detection, the Organization shall develop and implement appropriate activities to identify the occurrence of a Cybersecurity event. The Detect Function enables the timely discovery of Cybersecurity events. Examples of outcome Categories within this Function include detection of anomalies and Events; Continuous Monitoring of Security; and Detection Processes and Procedures.

5.1.1 Detection of Anomalies and Events

5.1.1.1 The Organization shall detect anomalous activities in a timely manner and understand the potential impact of the events;

5.1.1.2 The Organization shall define the standard baseline of an operating procedure that may include expected data flows for users and systems. The procedure shall be documented to serve the needful purpose for the users;

5.1.1.3 The Organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence;

5.1.1.4 The Organization shall comprehend the detected events to understand attack targets and methods;

5.1.1.5 The Organization shall aggregate and correlate event data from multiple sources and sensors;

5.1.1.6 The Organization shall determine the impact of events and establish incident alert thresholds;

5.1.1.7 The Organization shall maintain a comprehensive event log retention policy, ensuring all logs are securely stored for a defined period and are easily accessible for investigations and compliance audits;

5.1.1.8 The Organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence;

5.1.1.9 Privileges associated with each type of information system such as Operating Systems, Business Applications, Databases, and Network Elements shall be identified and documented;

5.1.1.10 Information involved in application service transactions shall be protected to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay;

5.1.1.11 The Organization shall address new threats and vulnerabilities for public-facing web applications in regular basis and ensure these applications are protected against known attacks.

5.1.2 Continuous Monitoring of Security

5.1.2.1 The Organization shall monitor information systems and assets at discrete intervals to identify Cybersecurity events and verify the effectiveness of protective measures;

5.1.2.2 The Organization shall monitor the network to detect potential Cybersecurity events;

5.1.2.3 The Organization shall collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets;

5.1.2.4 The Organization shall configure detailed audit logging for enterprise assets containing sensitive data, including event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation;

5.1.2.5 The Organization shall collect DNS query audit logs on enterprise assets, where appropriate and supported;

5.1.2.6 The Organization shall collect URL request audit logs on enterprise assets, where appropriate and supported;

5.1.2.7 The Organization shall collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals;

5.1.2.8 The Organization shall centralize, to the extent possible, audit log collection and retention across enterprise assets;

5.1.2.9 The Organization shall conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis;

5.1.2.10 The Organization shall deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported;

5.1.2.11 The Organization shall deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS);

5.1.2.12 The Organization shall collect network traffic flow logs and/or network traffic to review and alert upon from network devices;

5.1.2.13 The Organization shall tune security event alerting thresholds monthly, or more frequently;

5.1.2.14 The Organization shall observe unusual activities, and comprehend the possible consequence of occurrences;

5.1.2.15 The Organization shall monitor the physical environment to detect potential Cybersecurity events;

5.1.2.16 The Organization shall monitor personnel activities to detect potential Cybersecurity events;

5.1.2.17 The environment of the organization shall protect servers and workstations from malicious code by ensuring that approved anti-virus packages and Endpoint Detection and Response (EDR) are installed;

5.1.2.18 The Organization shall utilize an active discovery tool to identify assets connected to the enterprise's network and configure the active discovery tool to execute daily, or more frequently;

5.1.2.19 The Organization shall have mechanisms to detect unauthorized mobile code;

5.1.2.20 The Organization shall monitor external service provider activity to detect potential Cybersecurity events;

5.1.2.21 The Organization shall perform monitoring for unauthorized personnel, connections, devices, and software;

5.1.2.22 The Organization shall analyze, and record detected events to understand attack targets and methods;

5.1.2.23 The Organization shall assess information security events and it shall be decided if those are to be classified as information security incidents;

5.1.2.24 The Organization shall log sensitive data access, including modification and disposal;

5.1.2.25 The Organization shall perform Internal/ external vulnerability and penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment);

5.1.2.26 Privileged users associated with each type of information systems such as Operating systems, Business Applications, Databases, and Network Elements shall be identified and documented;

5.1.2.27 The Organization shall ensure that the access rights of the users to information assets are revoked within 24 hours (maximum 5 working days) of separation of their employment, contract, or agreement. This time period has also been governed by the evaluation of risk factors like the reason for termination, the current responsibilities of the user, and the value of assets currently accessible;

5.1.2.28 The Organization shall configure anti-malware software to automatically scan removable media;

5.1.2.29 The Organization shall use behavior-based anti-malware software;

5.1.2.30 The Organization shall ensure centralize security event alerting system for log correlation and analysis;

5.1.2.31 A log analytics platform shall be configured with security-relevant correlation alerts.

5.1.2.32 The Organization shall monitor service providers based on the service provider management policy of the organization. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, deep web and dark web monitoring.

5.1.3 Detection Processes and Procedures

5.1.3.1 The Organization shall maintain and test detection processes and procedures to ensure timely and adequate awareness of anomalous events;

5.1.3.2 The Organization shall define and allocate all information security roles and responsibilities to ensure accountability;

5.1.3.3 The Organization shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements;

5.1.3.4 The Organization shall regularly review information systems for compliance with the organization's information security policies and standards;

5.1.3.5 The Organization shall ensure knowledge of anomalous events, detection methods, and procedures are maintained and evaluated;

5.1.3.6 The Organization shall carry out the testing of security functionality during development;

5.1.3.7 The Organization shall communicate detection information to the appropriate parties;

5.1.3.8 The Organization shall continuously improve detection processes;

5.1.3.9 The Organization shall comply with the detection activities for all applicable requirements.

6 RESPOND

6.1 Introduction

The Organization shall 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. Examples of outcome categories within this function include Response Planning; Communications; Analysis; Mitigation; and Improvements.

6.1.1 Response Planning

6.1.1.1 The Organization shall execute and maintain response processes and procedures to ensure the response against detected Cybersecurity incidents;

6.1.1.2 The Organization shall respond to Cybersecurity incidents according to the plan with documented procedures;

6.1.1.3 Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents;

6.1.1.4 The Organization shall establish an incident management framework with the objective of restoring normal ICT service as quickly as possible following the incident with minimal impact on the business operations. The Organization has to respond rapidly to information security incidents according to the framework;

6.1.1.5 The Organization shall establish communication protocols to ensure timely and accurate updates are provided to internal teams, stakeholders and relevant authorities during a cyber incident;

6.1.1.6 The Organization shall conduct regular incident response drills, including both internal and external teams, to test the effectiveness of the response plan and identify areas for improvement;

6.1.1.7 Incidents shall be accorded with the appropriate severity level. As part of the incident analysis, the Organization may delegate the function of determining and assigning incident severity levels.

6.1.2 Communications

6.1.2.1 The Organization shall establish the management responsibilities and procedures to ensure a prompt, effective, and orderly response to Cybersecurity incidents;

6.1.2.2 The Organization shall maintain appropriate contacts with relevant authorities;

6.1.2.3 The Organization shall have an internal communication plan to coordinate the response activities that includes communication protocols for key internal stakeholders (e.g. relevant business units, Senior Management, Board of Directors, etc.), as appropriate;

6.1.2.4 The Organization shall have external communication plan to coordinate the response activities that includes communication protocols and draft pre-scripted communications for key external stakeholders (i.e. customers, critical service providers, BGD-CIRT team, Bangladesh Bank, etc.);

6.1.2.5 The Organization shall determine the need for internal and external communications relevant to the Cybersecurity management system including**:**

a. What to communicate?
b. When to communicate?
c. With whom to communicate?
d. Who shall communicate?
e. Which communication process shall be affected?

6.1.2.6 The Organization's personnel shall know their roles and order of operations when a response is needed;

6.1.2.7 The Organization shall share information consistent with response plans;

6.1.2.8 Voluntary information sharing occurs with external stakeholders to achieve broader Cybersecurity situational awareness;

6.1.2.9 The Organization shall share Cybersecurity information through BGD CIRT and Bangladesh Bank to external stakeholders to achieve broader Cybersecurity awareness.

6.1.3 Analysis

6.1.3.1 The Organization shall conduct analysis to ensure adequate response and support recovery activities;

6.1.3.2 The Organization shall investigate notifications from detection systems;

6.1.3.3 The Organization shall ensure that the impact of the incident is understood, forensics are performed and incidents are categorized consistent with response plans;

6.1.3.4 The Organization shall provide 24/7 identification and response capabilities for the Management of Cybersecurity;

6.1.3.5 The Organization shall establish Information Security Operation Center (ISOC);

6.1.3.6 The Organization shall introduce Cybersecurity Incident Reporting (CSIR) system;

6.1.3.7 The Organization shall prepare and maintain a baseline of Cybersecurity and Resilience requirements;

6.1.3.8 The Organization shall assign specific roles and responsibilities for the Management of Cybersecurity, and these individuals have to have sufficient delegated operational authorities;

6.1.3.9 The Cybersecurity specialists are subject to enhanced background and security checks;

6.1.3.10 The Organization shall have a Computer Incident Response Team (CIRT) with a specific TOR;

6.1.3.11 The Organization shall have a cyber-incident investigation team to investigate any incident;

6.1.3.12 The Organization shall implement the following security solutions (but not limited to) and provides automated updates:

a. Security information and event management (SIEM)
b. Privileged Access Management (PAM)
c. Anti APT (Advanced Persistent Threat)
d. Intrusion Protection System (IPS)
e. Intrusion Detection System (IDS)
f. Web Application Firewall (WAF)
g. Next-Generation Firewall
h. Web gateway security
i. DDOS Protection
j. Content Filtering
k. E-mail Security
l. Web Proxy
m. API Protection
n. Deception/Decoy
o. Active Directory Security
p. Cloud-Native Application Protection Platform (CNAPP)
q. Zero Day Attack Prevention and Detection with Sandboxing
r. Anti-Malware / Anti Ransom ware / Anti-spyware /Anti-spam
s. Respective technologies Information Security Operation Center (ISOC), etc.;

6.1.3.13 The Organization shall establish and implement firewall and router configuration standards that include the following:

a. A formal process for approving and testing all network connections and changes to the firewall and router configurations;
b. Current network diagram that identifies all connections between the data environment and other networks, including any wireless networks;
c. Current diagram that shows all data flows across systems and networks;

d. Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone;
e. Description of groups, roles, and responsibilities for management of network components;
f. Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure;
g. Requirement to review firewall and router rule sets at least once in every quarter or after any critical changes happened;
h. East-west traffic along with north-south traffic should be inspected through firewall;
i. North-South traffic for both MZ and DMZ should be inspected twice.

6.1.3.14 The Organization shall assess the overall security of the network to identify vulnerabilities;

6.1.3.15 The Organization shall rapidly isolate, restrict or shut down compromised devices from the network;

6.1.3.16 The Organization must log system administrators, privileged users, and other system operators' operations, and the logs must be safeguarded and examined regularly;

6.1.3.17 The Organization shall review the following at least daily:

a. All security events;
b. Logs of all system components that store, process, or transmit Card Holder Data (CHD) and/or Sensitive Authentication Data (SAD);
c. Logs of all critical system components;
d. Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

6.1.4 Mitigation

6.1.4.1 The Organization shall mitigate Cybersecurity incidents by the documented procedures;

6.1.4.2 The Organization shall perform activities to prevent the expansion of an event, mitigate its effects, and eradicate the incident;

6.1.4.3 The Organization shall ensure that the incidents are contained and mitigated;

6.1.4.4 The Organization shall mitigate and document newly identified vulnerabilities as accepted risks;

6.1.4.5 The Organization shall perform activities to prevent the expansion of an event, mitigate its effects, and resolve the incident;

6.1.4.6 The Organization shall obtain information about technical vulnerabilities of information systems in a timely fashion. The organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken to address the associated risk;

6.1.4.7 Procedures for working in secure areas shall be designed and applied;

6.1.4.8 The Organization shall measure the level of cyber attack by implementing shielding controls/quarantining the affected devices/systems;

6.1.4.9 The Organization shall implement the policy and framework for aligning Security Operation Centre, Incident Response, and Digital Forensics to reduce the business downtime.

6.1.5 Continuous Improvements

6.1.5.1 The Organization shall improve organizational response activities by incorporating lessons learned from current and previous detection/response activities;

6.1.5.2 The Organization shall incorporate lessons learned into response plans and update response strategies;

6.1.5.3 The Organization shall update and review response strategies;

6.1.5.4 The Organization shall regularly review and update its inventory of critical systems and assets to ensure that response priorities reflect any changes in business or technological infrastructure.

7 RECOVERY

7.1 Introduction

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 of a Cybersecurity incident. Examples of outcome Categories within this Function include Recovery Planning; Improvements; and Communications.

7.1.1 Recovery Planning

7.1.1.1 The Organization shall execute and maintain recovery processes and procedures to ensure the timely restoration of systems or assets affected by Cybersecurity events;

7.1.1.2 The Organization shall maintain adequate insurance coverage or risk coverage fund so that costs of loss and/or damage of the assets can be mitigated due to cyber attacks;

7.1.1.3 The Organization shall execute the recovery plan during or after a Cybersecurity events;

7.1.1.4 The Organization shall set up BCP/DRP capabilities that will adequately and effectively support the cyber resilience objectives;

7.1.1.5 The Organization shall design and plan to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring the security of processes and the protection of data.

7.1.1.6 The Organization shall ensure such capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative and coordinated resilience testing that meets the recovery time objectives;

7.1.1.7 The Organization shall define incidents, methods of detection, methods of reporting incidents by employees, vendors, and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel managing/handling such incidents, provide specialized training to such personnel, post-incident review and periodically test incident response plans;

7.1.1.8 The Organization shall manage and analyze audit logs systematically to detect, understand and/or recover from an attack;

7.1.1.9 The Organization shall establish and maintain a data recovery process. In the process, the scope of data recovery activities, recovery prioritization, and the

security of backup data shall be addressed. The documentation shall be reviewed and updated annually, or when significant enterprise changes occur.

7.1.1.10 The Organization shall perform automated backups of in-scope enterprise assets. Moreover, the Organization shall run backups weekly, or more frequently, based on the sensitivity and criticality of the data;

7.1.1.11 The Organization shall establish and maintain an isolated instance of recovery data. Example implementations include, version-controlling backup destinations through offline, cloud, or off-site systems or services;

7.1.1.12 The Organization shall test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets;

7.1.1.13 The Organization shall plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision-making, and workflows. Conduct testing on an annual basis, at a minimum;

7.1.1.14 The Organization shall conduct post-incident reviews. Post-incident reviews shall be able to prevent incident recurrence by identifying lessons learned and follow-up action;

7.1.1.15 The Organization shall establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include abnormal activity, security vulnerability, security weakness, data breaches, privacy incidents, etc.

7.1.1.16 The Organization shall document and communicate strategies to respond to advanced attacks containing ransomware/cyber extortion, data destruction, DDOS, etc.;

7.1.1.17 The Organization shall measure the level of cyber attack by implementing shielding controls/quarantining the affected devices/systems;

7.1.1.18 The Organization shall ensure that a recovery plan is executed during or after a cyber-security incident;

7.1.1.19 The Organization shall manage and analyze audit logs systematically to detect, understand or recover from an attack.

7.1.2 Continuous Improvement Metrics and KPIs

7.1.2.1 The Organization shall improve organizational recovery activities and capabilities by incorporating lessons learned from current and previous recovery activities;

7.1.2.2 The Organization shall incorporate lessons learned into recovery plans and update recovery strategies;

7.1.2.3 The Organization shall update and review recovery strategies;

7.1.2.4 The Organization shall introduce Key Performance Indicators (KPI) for tracking continuous improvement, such as

a. Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to incidents;
b. Reduction of critical vulnerabilities over time;
c. Frequency and completion rates of Cybersecurity awareness training.

7.1.3 Communications

7.1.3.1 Restoration activities shall be coordinated with internal and external parties (e.g. Coordinating centers, Internet Service Providers, owners of attacking systems, victims, CIRTs, and vendors);

7.1.3.2 The Organization shall communicate to internal and external stakeholders as well as executive and management teams to perform Recovery activities;

7.1.3.3 The Organization shall communicate with the regulatory authority to perform recovery activities in the event of major or critical cyber incident;

7.1.3.4 The Organization shall manage public relations;

8 Reporting

8.1 Introduction

Cyber incident reporting is necessary when an organization that has been affected by a cyber attack, data breach, data leak, or any situation where sensitive information was exposed. It is necessary to report the incident to the proper parties, which typically include stakeholders, law enforcement, affected customers, business partners, and government officials.

Because cyber threats continue to grow in sophistication and effectiveness, cyber incident reporting is not only important, but also necessary for other organizations to learn from and prevent making the same mistakes. Many governing bodies and federal governments around the world have begun to require cyber incident reporting documenting the type of attacks used, the source of the attacks, and how the attacks occurred to better understand the threat landscape.

8.1.1 Communications

8.1.1.1 The Organization shall maintain appropriate contacts with relevant authorities;

8.1.1.2 The Organization shall have an internal communication plan for sharing the reports to key internal stakeholders (e.g. relevant business units, Senior Management, Board of Directors, etc.), as appropriate;

8.1.1.3 The Organization shall have a process to send the report of cyber incidents to the regulatory authority;

8.1.1.4 The Organization shall have external communication plan for sharing the reports to key external stakeholders (i.e. customers, critical service providers, BGD-CIRT, Bangladesh Bank etc.);

8.1.1.5 The Organization shall report events consistent with established criteria;

8.1.1.6 The Organization shall share cyber incident report to BGD-CIRT, Bangladesh Bank, external stakeholders to achieve broader Cybersecurity awareness;

8.1.1.7 The Organization shall deliver the right message content to the right audience using the most effective communication channels;

8.1.1.8 Since the target groups obtain information from a variety of sources, more than one communication channel could be used to engage them successfully.

a. Common website developed with content from all stakeholders;
b. Online training modules and demos hosted on this site;
c. Interactive guidance in the form of helpline;
d. Customer meets and interactive sessions with specialists;
e. Talk shows on television/radio.

8.1.2 Reporting Criteria

8.1.2.1 For any critical cyber incident, the organization shall report to internal (e.g., relevant business units, senior management, Board of Directors etc.) and external stakeholders (i.e., customers, critical service providers, BGD-CIRT, Bangladesh Bank etc.) within 72 hours from the time of occurrence;

8.1.2.2 The Organization shall understand the importance of Incident reporting because it provides a way for organizations and businesses to document, respond, and learn from a cyber attack. Incident reporting should be part of every organization's security program as part of the incident response process;

8.1.2.3 When information about cyber incidents is shared quickly, the organization may use this information to render assistance and provide warning to prevent other organizations from falling victim to a similar incident omitting sensitive information. This information is also critical to identifying trends that can help efforts to protect the homeland.

8.1.3 Cybersecurity Audit

A Cybersecurity audit involves a comprehensive analysis and review of the organization's IT infrastructure. It detects vulnerabilities and threats, displaying weak links and high-risk practices. Significant benefits of Information Security audits are: risk assessment, vulnerability identification and strengthened security measures. It is very important to perform Cybersecurity audit in regular basis at least once in a year and after any incident or cyber attack happened.

8.1.3.1 The Organization shall define the specific goals and objectives of the Cybersecurity audit. For example(but not limited to):

a. Evaluating network security controls;
b. Assessing the effectiveness of access management processes;
c. Identifying potential weaknesses in the incident response plan;
d. Evaluating the effectiveness of monitoring processes and logging controls to identify potential gaps;
e. Reviewing and conducting thorough testing of Disaster Recovery and Business Continuity plans at least once annually.

8.1.3.2 Cybersecurity audits ensure a 360-degree in-depth audit of the organization’s security posture. It aims to identify vulnerabilities, risks, and threats that may affect the organization. These audits cover various areas, including:

a. Data Security – involves reviewing network access control, encryption use, data security at rest, and transmissions and data sharing mechanism with third party;
b. Operational Security – involves a review of security policies, procedures, and controls;

c. Network Security – involves reviewing of network and security controls, anti-virus configurations, security monitoring capabilities, etc.;
d. System Security – this review covers hardening processes, patching processes, privileged account management, role-based access, etc.;
e. Physical Security – a review that covers disk encryption, role-based access controls, biometric data, multifactor authentication, etc.

8.1.3.3 The Organization shall understand other significant benefits of information security and Cybersecurity audits:
a. Risk assessment and vulnerability identification;
b. Strengthened security measures;
c. Compliance with regulations and standards;
d. Incident response preparedness;
e. Safeguarding sensitive data and customer trust;
f. Proactive threat detection and prevention.

8.1.3.4 The Organization shall conduct audit by either external Cybersecurity services companies or internal teams. The audit shall be conducted at least once in a year as well as, after any security breach;

8.1.3.5 In case of external security audit, the Organization shall find the right and affordable auditing company, set expectations for auditors, submit relevant and accurate information, and implement suggested changes.

8.1.4 Lesson-Learned

8.1.4.1 The primary and foremost objective of any cyber incident/ cyber attack lesson learned is to educate users (employees and customers) on their responsibility to protect the confidentiality, availability, and integrity of the organization's information;

8.1.4.2 The Organization shall use this lesson-learned to educate users (employees and customers) to equipped themselves about self-help by providing proper employee education and customer awareness;

8.1.4.3 The Organization shall not be tempted to let multiple known security risks sit unresolved because the organization thinks that there is another layer of security in place;

8.1.4.4 The Organization shall never rely on MFA (multifactor authentication) alone to protect critical assets. The Organization shall be aware of that the hackers may compromise MFA on occasion and target the highest value security assets;

8.1.4.5 The Organization shall understand that the threats were not necessarily new;

8.1.4.6 The Organization shall understand many organizations were still vulnerable;

8.1.4.7 The Organization shall understand that back up the organizational data and information is important;

8.1.4.8 The Organization shall report incidents and take the proper response steps immediately, if affected,

8.1.4.9 The Organization shall understand that paying the ransom does not guarantee encrypted data and information of the organization will be returned.

8.1.5 Post Incident Analysis

Post-incident analysis, the final stage in the incident response lifecycle, plays a pivotal role in the pursuit of cyber resilience. Post-incident reviews (PIRs) bring people and teams together to discuss the details of an incident: why it happened, what impact it had, what actions were taken to resolve it, and how the team can prevent it from happening again. This analysis goes beyond merely containing the incident; it seeks to uncover the root causes, vulnerabilities, and procedural gaps that contributed to the breach.

8.1.5.1 This process usually includes a meeting with key stakeholders and personnel to understand the incident in greater detail and to learn important lessons from it. The analysis include the following questions:

a. Exactly what happened, and at what times?
b. How well did staff and management perform in dealing with the incident?
c. Were the documented procedures followed?
d. Were they adequate?
e. What information was needed sooner?
f. Were any steps or actions taken that might have inhibited the recovery?
g. What would the staff and management do differently the next time a similar incident occurs?
h. How could information sharing with other organizations have been improved?
i. What corrective actions can prevent similar incidents in the future?
j. What precursors or indicators should be watched for in the future to detect similar incidents?
k. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

9 CONCLUSION

Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), personal information, intellectual property, data, and governmental and industry information systems. Without a Cybersecurity program, the Organization cannot defend itself against data breach campaigns, which makes it an irresistible target for cybercriminals.

Every organization needs to manage Cybersecurity risk as a part of doing business, whether it is in industry, government or academia. It is critical to their resilience and to our nation's economic security. This document represents an initial, high-level summary of the Cybersecurity responses. This Framework for improving Critical Cybersecurity Infrastructure is released in March 2026 after extensive public engagement and collaboration from different banks and Financial Institutions of the country. The Framework serves as a prominent resource to manage Cybersecurity risks holistically across an organization. This framework was intended to be a living document that is refined, improved, and evolves over time to keep pace with technology and threat trends, integrate lessons learned, and move best practice to common practice.

In order to keep pace with the ever-evolving Cybersecurity landscape and to help organizations more easily and effectively manage Cybersecurity risk, Bangladesh Bank will review this Framework time to time.

Appendix A: CYBERSECURITY SOLUTIONS AND TECHNOLOGIES

The following solutions and Technologies shall be implemented for monitoring by SOC (The list is illustrative and not exhaustive):

1. Security information and event management (SIEM)
2. SYSLOG Server
3. Privileged Access Management (PAM)
4. File Integrity Monitoring (FIM)
5. Intrusion detection system (IDS)/ Intrusion prevention system (IPS)
6. Anti APT (Advanced Persistent Threat)
7. Threat and Vulnerability management
8. Threat Intelligence
9. Web Application firewall
10. Email Security Appliance (ESA)
11. Web Security Appliance (WSA)
12. API Security
13. Security Management Appliance (SMA)
14. SOAR: Security Orchestration, Automation, and Response
15. Firewalls and Unified Threat Management (UTM)
16. Anti-Virus/Total Protection
17. DLP-End points and Gateway
18. DDoS Protection
19. Network access control (NAC)
20. Network Detection and Response (NDR)
21. Network Proxy
22. ATM Security
23. Compromise Assessment
24. Database Activity Monitoring (DAM)
25. Governance Risk and Compliance (GRC) solution
26. PKI, SSL and SSO Infrastructure
27. Mobile Device Management (MDM) Platform/solution
28. Cloud Security and Virtualization environment
29. Digital Risk Management/Brand Protection/Deep-Dark Web monitoring
30. Any other security solution as deemed required by the organization to ensure confidentiality, integrity and availability of data etc.

Appendix B: SOLUTION DETAILS

Domain coverage	Solution details
Identity and Access Management	• Identity and access management solution • Privilege identity/ access management (PIM/PAM)
Data Leakage Prevention	• Network DLP • Email DLP • Endpoint DLP
Endpoint Security	• End-user disk encryption • Desktop Firewall • Anti-virus/Anti-Malware
Host Security	• Host Intrusion Prevention System • File Integrity monitoring solution
Web Security	• Web Access Security / Web Application Firewall • 2-factor authentication for Internet and mobile banking (can be OTP, PW, Grid combo)
Cloud Security	• Service Provider's application based security solutions • Cloud network security controls • Firewalls • Web Access Security / Web Application Firewall • Encryption solutions • Anti-virus/Anti-Malware
Perimeter Security	• DDoS Protection • Network Intrusion Prevention System • Perimeter Firewall • Remote Access/VPNs
Handheld / Mobile Device Security	• Mobile Device Management solution
Patch management	• Patch management
Security Orchestration, Automation, and Response	• SOAR is designed to automate the response process by gathering alerts, managing cases, and responding to the alerts generated by SIEM. Using SOAR, security teams can integrate with security alerts and create adaptive, automated incident response workflows. This gives Security Operations the ability to prioritize threats and deliver faster results.

Appendix C: SAMPLE CHECKLIST FOR CYBERSECURITY ASSESSMENT

Sl. No.	Question	Yes	No
	Documented Security Procedures and Accountability		
1	Have you created security policies commensurate with the size and culture of the organization?	☐	☐
2	Are security policies documented and updated?	☐	☐
3	Is maintaining the security of the organization made part of each employee's job description?	☐	☐
4	Are all employees required to sign confidentiality agreements?	☐	☐
5	Are all contractors, facility managers, couriers, maintenance companies, cleaners explicitly informed about the organizations policies and standards that apply to their activities?	☐	☐
6	Are legal notices posted on log-on and authentication screens warning that unauthorized access or use constitutes an illegal intrusion?	☐	☐
7	Does the organization restrict employee access to critical systems and information?	☐	☐
8	Does the Organization classify data, identifying sensitive versus non sensitive data?	☐	☐
9	Are maintenance and cleaning staffs prevented from entering areas unsupervised which contain mildly sensitive systems and information and above?	☐	☐
10	Are employees prohibited from installing personal, or unauthorized software on their organization supplied computer, laptop, tablet, smart phone or any other device?	☐	☐
11	Are employees required to have a 'strong' password on personal smart phones and other devices on which they have access to company emails or other sensitive information?	☐	☐
12	Do the Organizations policies define the proper use of email, internet access, instant messaging by employees?	☐	☐
13	Are employees prohibited from sharing passwords and allowing other employees to use their computers and portable devices?	☐	☐
14	Are there procedures in place to prevent computers from being left in a logged-on state, however briefly?	☐	☐
15	Is the employee who is responsible for a given piece of information equipment required to oversee the security of that equipment?	☐	☐
16	Is each piece of equipment tagged using a permanent identifier and or the serial number recorded to determine who is entrusted with the piece of equipment?	☐	☐
17	Are there measures to prevent employees from leaving the business premises with sensitive information carried on USB or other media devices?	☐	☐
18	Are employees provided sufficient incentives to report security breaches and improper security practices and at the same time protected from retribution or blame from making such a report?	☐	☐

Sl. No.	Question	Yes	No
19	Is there a procedure in place to immediately revoke all passwords and/or prevent access to company property, data intellectual property, customer records, restricted physical areas and to any supplier or customer of the organization?	☐	☐
20	Are employees prohibited from allowing other staffs or any other person to use their swipe card, keys, pin numbers and the like to gain access to information facilities or systems?	☐	☐
Backup Procedures and Security			
21	Are the operating systems, programs and operating information backed up as well as the data/records?	☐	☐
22	Is the data being backed up at a frequency appropriate to its sensitivity and importance to the organization?	☐	☐
23	Does the back-up procedure include checking the data for hostile code such as Trojan horses or viruses?	☐	☐
24	If the information being backed up is proprietary or sensitive, is the information encrypted and stored as such during the back-up process?	☐	☐
25	Are all copies of back-ups protected from loss by fire, theft and accidental damage?	☐	☐
26	Are there any secured procedures for destroying or reusing the media, when it is no longer required?	☐	☐
27	Are there multiple backups so that if one is lost or corrupted, the system could still be restored?	☐	☐
28	Are the backups being retained long enough so that there would still be an uncorrupted copy if the data was gradually being corrupted or the system was shut down as part of a ransom or other malicious attack?	☐	☐
29	Are all relevant logs of activity backed up and securely stored to prevent alteration?	☐	☐
30	Are the configurations of switches and routers backed up on a regular basis?	☐	☐
31	Are the backups regularly stored at a physically remote location?	☐	☐
32	Are the backups regularly tested to ensure they are working as they should?	☐	☐
33	Are there procedures to deal with the loss or theft of unencrypted backup data that is proprietary or of a sensitive nature?	☐	☐
Security of Hardware, Data and Records			
34	Are all electronic equipments (hardware and software) listed on an accurate inventory listing and where appropriate housed in a secure area?	☐	☐
35	Are there documented, quick and easy, procedures for updating the inventory whenever it is to be moved or the person allocated to use/protect it changes?	☐	☐
36	Is each piece of equipment labeled with a bar code or other identifier for easy tracking?	☐	☐
37	Is there a procedure for the removal and destruction of hard discs or other media when the equipment reaches the end of its useful life or is otherwise taken out of service permanently?	☐	☐
38	Do you have procedures for disposing of waste material?	☐	☐

Sl. No.	Question	Yes	No
39	Where equipment is being reassigned to a different employee, is there a procedure in place to ensure that sensitive information is not left on the machine that would not normally be accessible by the employee entrusted with the equipment moving forward?	☐	☐
40	Are there periodic checks to ensure that the equipment is where it is reported to be?	☐	☐
41	Do you have policies covering laptop security (e.g. cable lock or secure storage)?	☐	☐
42	Are especially important items of electronic equipment housed in a secure datacenter, room or cabinet?	☐	☐
43	Are their physical barriers of access to the equipment commensurate to the value of the equipment and the data contained in it?	☐	☐
44	Do you have a process for effectively cutting off access to facilities and information systems when an employee/contractor terminates employment?	☐	☐
45	Are there clear and rigorously enforced restrictions on who has access to the datacenter, computer room or cabinets?	☐	☐
46	Do your policies and procedures specify the methods used to control physical access to your secure areas, such as door locks, access control systems, security officers, or video monitoring?	☐	☐
47	Are there strict policies outlining the procedures for afterhours access to the datacenter, or computer room by personnel such as custodians?	☐	☐
48	Does the datacenter or main computer room have a sign-in procedure that is used to record non-employees into the restricted space?	☐	☐
49	Are datacenter, data rooms and data cabinets protected by adequate fire and burglary detectors and or CCTV and or fire suppression systems commensurate with the cost of the loss of the equipment, data or records?	☐	☐
50	Is there sufficient heating and cooling to the datacenter/computer room to maintain a consistent safe operating temperature for the electronic equipment?	☐	☐
51	Is the electronic equipment protected from moisture or excessive humidity, dust, smoke, chemical fumes or other potentially damaging substances?	☐	☐
52	Is there a risk of water entry to any area housing critical equipment or records from water pipes, hot water systems, waste pipes, storm water pipes, box gutters or sprinkler systems?	☐	☐
53	Is physical access to the console interfaces of security systems such as those used to manage firewalls, CCTV and intrusion systems, restricted to authorized users?	☐	☐
54	Do you ensure users have anti-virus software loaded and active on systems?	☐	☐
55	Are documents that contain sensitive information secured or otherwise protected from unauthorized printing?	☐	☐
56	Does the company have a documented and enforced procedure for the safe disposal of paper records that are no longer required?	☐	☐
57	Is waste paper binned or shredded?	☐	☐

Sl. No.	Question	Yes	No
58	Are there sufficiently rigorous policies and procedures governing the use of removable magnetic media, such as USB devices?	☐	☐
59	Are there sufficiently rigorous procedures to restrict unauthorized access to back-up media?	☐	☐
Security of Access Ports and Communication Lines			
60	Are unused network or telecommunication access points physically disabled to prevent unauthorized access?	☐	☐
61	Where the network and telecommunications ports are not disabled are there procedures to monitor for unauthorized access to these ports?	☐	☐
62	Are there physical barriers to protect the network cables running to and from the equipment to reduce accidental or deliberate damage?	☐	☐
Training on Security Procedures			
63	Are all staffs provided with periodic training on the organization's security policies with an explanation as to why the policies are important and compliance will be enforced?	☐	☐
64	Are all staffs provided with periodic training on basic cyber-security hygiene practice?	☐	☐
65	Are there enough training facilities provided for information security division/department/unit staff to ensure developing expert cyber-security specialist?	☐	☐
66	Are employees trained/warned on the importance of keeping watch and or securing laptops and other portable information devices when taking them outside the workplace?	☐	☐
67	Are employees trained to use 'strong' passwords and not to base passwords on biographical details that may be publicly available?	☐	☐
68	Are there mechanisms developed for assessing the information security and Cybersecurity skill level of all staffs?	☐	☐
69	Are there mechanisms developed to ensure Cybersecurity awareness is provided to all employees and other relevant stakeholders?	☐	☐
