CENTRAL BANK OF JORDAN

FINANCIAL CYBER EMERGENCY RESPONSE TEAM

Cybersecurity Framework for Jordan Financial Sector

Version 1.0 – July, 2021

Foreword

It is quite evident that the financial industry is going through a revolutionary phase at which technology and telecommunications are the basic infrastructure for this new financial world order. Therefore, banks and financial institutions are keen to adopt and leverage on digital financial services to be more competitive, reduce cost, and achieve institutional efficiency to keep up and survive the new playground.

To ensure safety and smooth operations of finance in this new world order, cybersecurity becomes more and more critical. As the industry is growing and cybersecurity threats and attacks are developing too; serious efforts must be employed to create powerful cyber-resilient infrastructure.

Central Bank of Jordan realized this and took a leading role in developing this Cybersecurity Framework which offers a better understanding for the threat landscape, and outlines the requirements necessary to ensure cyber resiliency. CBJ will collaborate with the industry members to meet the objectives stated in this framework.

With great synergy and participation of all our partners in the financial sector, this framework will be one of our safeguards which eventually shall ensure the sector's resiliency, propel financial and economic development, and strengthen our national reputation on a regional and international levels, thus attracting investments and innovation.

Dr. Ziad Fariz

The Governor of Central Bank of Jordan

Table of Contents

Definitions

Term	Definition
Accountability	The property of being able to trace activities on a system to individuals who may then be held responsible for their actions. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Advanced Persistent Threat (APT)	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges
Availability	Ensuring timely and reliable access to and use of information. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Baseline	A set of minimum requirements to be met, and form the base for measurement
BYOD	Bring Your Own Device (BYOD) refers to the practice of performing work-related activities on personally owned devices
Criticality	A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Cyber Resiliency	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Cyber Risk	Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system. (NISTIR 7298r3 Glossary of Key Information Security Terms)

Cyber Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Data Confidentiality	The property that data or information is not made available or disclosed to unauthorized persons or processes. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Data Integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Data Privacy	The governance for proper handling of sensitive data during collection, using, sharing and storing, in a way that grant the right to a party to maintain control over and confidentiality of information about itself
Data Security	A set of security objectives to protect data from unauthorized access, use, disclosure, disruption, modification, or destruction in order to maintain confidentiality, integrity, and availability
Digital Boarding	The practice of signing up for a bank account or other banking service entirely online or via mobile with no physical presence
Disaster	An incident, either man-made or natural, sudden or progressive, the impact of which is such that the affected organization must respond through exceptional measures
Event	Any observable occurrence in a network or information technology, service or system
Financial Transaction	A communication carried out between at least two parties to exchange a value of asset, and result in changes in the status of the finances of the parties
Governance	A set of processes that ensures that assets are formally managed throughout the enterprise
Guideline	A set of recommendations or goals that can be used when there are no specific standards/procedures in place, or they do not apply.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Information Asset	Any resource that the entity possess or employs to support information-related activities
Information Protection	A set of security policies, processes, and procedures to manage protection of information systems and assets.
Online Banking	Mobile-based or web-based banking in which customers reach traditional banking services over Internet (from desktops, tablets, mobiles, …)

Policy	Statements, rules or assertions that specify the correct or expected behavior of an entity. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Portable Devices	Computing devices include laptops, mobiles, and tablets that are owned by the entity, easily carried and moved, and allowed to connect to entity's network
Procedure	Set of activities or steps done to achieve business process goals or apply policy
Relevant Stakeholders	Internal employees who are empowered by the board of directors or senior management to independently make decisions
Removable Media	Portable storage device that are connected to information systems to provide data storage
Security Standard	A set of published specifications that are designed to enhance the organizational, sectoral, national and international security posture
Senior Manager	A role at the highest level of management who manage, direct, and control within the organization
Sensitivity	A measure of the degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components. (NISTIR 7298r3 Glossary of Key Information Security Terms)
Strategy	A high-level and long-term plan of actions designed to achieve the desired objectives
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NISTIR 7298r3 Glossary of Key Information Security Terms)

Introduction

The rapid growth of technologies and communications presents significant opportunities. Digitalizing business processes and digitizing access to services led to enhance performance, speed up overall servicing time and achieving more accuracy and cost optimization. Processing huge amounts of data about markets, consumers and beneficiaries is the main key behind drawing the future of business and investment, making information the most valuable asset.

Technological revolution, adoption and digital communications upon institutions open up the window for new types of risks and threats. Arising cyber threats are significant risks that can compromise the benefits of digital transformation. Such risks need to be addressed in order to ensure safe and secured technology and communication systems, leading to a safe and sound digital environment for the financial sector, while maintaining high standard cyber security measures. This will ultimately achieve the goals of having a safe and sound digital financial atmosphere.

As a pillar of the Financial Sector Cybersecurity Strategy of Jordan (2021 – 2023), this framework is laid out to put in place the right measures to mitigate and manage cyber risks in a structured and effective manner.

By this framework, it is going beyond the process of compliance and review through allocating cybersecurity capabilities in terms of people, technologies and processes. One of the main aims of this framework is ensuring the management and handling of cyber incident capabilities, and ensuring the commitment of CBJ-regulated entities by applying the right, efficient and effective control in the right place and the right time by following risk-based approach. The second goal of this framework is ensuring information sharing within the industry as banks and financial institutions share common vulnerabilities and threats landscape; and the massive sectoral impact that a local incident can cause to the whole sector.

Scope

The scope of the framework covers cybersecurity controls and practices that are applicable to banking industry, and include – but not limited to –:

- Cyber governance and risk management.
- Cybersecurity strategies, policies, procedures and standards.
- People qualification
- IT systems, infrastructures, networks and processes.
- Electronic service delivery channels
- External dependencies on third-parties.

The framework provides related cybersecurity baselines for CBJ-regulated entities, their subsidiaries, third parties and customers. Hereinafter, scoped entity referred to as “entity”

Responsibilities

The framework is published and owned by CBJ. FinCERT has the responsibility for assessing the implementation of this framework, and entities are responsible for adopting and implementing the framework.

By its role, FinCERT is responsible for protecting the confidentiality of classified information gathered about member entities, and any breach shall be handled as an incident.

Target Audience

This framework is intended for all roles inside the entity that are involved in defining, implementing and reviewing cybersecurity controls, as well as managing cybersecurity processes. These roles include, but not limited to, the board of directors, senior and executive management, business and information assets owners, as well as information security and information technology personnel.

Framework Structure – A Risk-Based Approach

This framework establishes cybersecurity baselines in the form of minimum considerations and requirements that entities have to implement (where applicable) to improve the overall financial sector cybersecurity posture. By this framework; it's assumed that entities shall implement requirements to reduce cyber risk exposure by focusing on the actual quantified and prioritized risks. This approach provides the entity a realistic view of the missing cybersecurity capabilities, and help in avoiding misleading and inefficient use of resources due to performing compliance-based risk reduction before evaluating actual risks.

The baselines have been developed and designed with appropriate consideration to relevant CBJ regulations, instructions and guidelines, as well as international best practices and regulations, standards, frameworks, directives and guidelines such as National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Payment Card Industry (PCI), SWIFT Customer Security Controls Framework (CSCF), and Information Systems Audit and Control Association (ISACA). Furthermore, the baselines have been guided by advisories, benchmarks and assessment methodologies and tools developed and published by American and European agencies such as Federated Financial Institution Examination Council (FFIEC).

The Framework is structured into five main parts:

PART1: Cybersecurity Governance and Management Controls

PART2: Cybersecurity Technical and Operational Controls

PART3: Crisis Management and Contingency Planning

PART4: Collaboration

PART5: Assessment

Each part consists of multiple sub-parts that organize the different cybersecurity topics. Each topic states the purpose and expectations to achieve as a part of a comprehensive risk management program.

"has to", "have to", "need", "require", "shall", and "must" in a context of stating control indicates that the control is considered as a minimum expectation to be achieved and fulfilled to reduce an identified and evaluated cyber risk.

"should", "could", "may", "might", "can" in a context of stating control indicates that the control is considered as a recommendation unless mandated by any other industry practices or regulations.

PART1 Cybersecurity Governance and Management Controls

A. Cybersecurity Oversight and Governance

A.1. Roles and Responsibilities

Entities have to adopt and ingrain a governance model into the organizational structure for implementing and managing the cybersecurity program with the following roles and responsibilities:

Board of Directors

Board of directors is the ultimate accountable for cybersecurity in the organization and mainly responsible for:

1. Approving strategic goals, business objectives, and endorsing the governance of cybersecurity.
2. Approving the cyber risk appetite as part of the overall risk appetite. This is to ensure that overall cyber risk is within the acceptable range.
3. Approving and overseeing the cybersecurity program, strategy and policy to manage cyber risks.
4. Ensuring the implementation of the cybersecurity program, as well as the acceptance and compliance with released policies, standards and procedures.
5. Approving cyber risk management processes.
6. Assigning cybersecurity-related roles and responsibilities.
7. Being supportive and engaged in cyber risk resiliency and posture assessments, sectoral evolving trends of cyber risks and threats and any cybersecurity-related initiatives.
8. Being aware of legal and regulatory implications of cyber risks.
9. Supporting the culture of awareness of cybersecurity in the organization.
10. Allocating adequate budget and resources for fulfilling cybersecurity requirements.

Cybersecurity Steering Committee

1. Board of directors can delegate cybersecurity-related responsibilities to a dedicated cybersecurity steering committee that is established and mandated by the board. The committee structure shall be:
   1.1 Headed by the Chief Executive Officer (CEO).
   1.2 Consisting of the following members:
      1.2.1 The accountable manager of cybersecurity function.
      1.2.2 Relevant department executive managers (e.g. Chief Information Officer, Chief Operating Officer, Risk Officer, Compliance Officer, heads of critical business departments).
      1.1.1 Head of Internal Audit as an observer.

2. Committee charter should be developed and approved by the board of directors, and should include at least:
   2.1 The committee objectives.
   2.2 The frequency and the quorum of meetings. Number of meetings should not be less than four annually.
3. In addition to board delegated responsibilities; the committee is responsible for:
   3.1 Reviewing and communicating cyber risk appetite to the board and other relevant stakeholders.
   3.2 Reviewing cybersecurity program, strategy, and policy, and ensuring their support for business objectives.
   3.3 Reviewing and communicating cyber risk management processes, key risk indicators and key performance indicators of cybersecurity program.
   3.4 Reviewing and communicating cyber risk resiliency and posture assessments reports.
   3.5 Ensuring the availability of adequate cybersecurity resources.
   3.6 Reviewing cybersecurity awareness programs and the outcomes of the effectiveness measurement.
   3.7 Reviewing sectoral evolving trends of cyber risks and threats and supporting cybersecurity-related initiatives.

Information and Cyber Security Management

1. The entity must institutionalize the cybersecurity function in a way that ensures appropriate level of independency of any other role that might conflict with cybersecurity program and objectives, including reporting path, budget and resources. Cybersecurity function shall:
   1.1 Develop and maintain the cybersecurity program including cyber risk management processes, as well as cybersecurity-related strategy, policy, standards, procedures, guidelines and baselines, key risk indicators and key performance indicators for the cybersecurity program.
   1.2 Develop the approach for engaging cybersecurity function in the organization processes at all levels.
   1.3 Manage cyber risk assessments, propose mitigation controls and procedures in a business context, and define cybersecurity requirements for new and ongoing projects and business activities, as well as managing the process of information and system classification.
   1.4 Manage the implementation of the cybersecurity program.
   1.5 Assess the adequacy of controls and approve exceptions considering the stated cyber risk appetite and enforced regulations.
   1.6 Monitor, analyze and communicate information on security alerts and events.

1.7 Establish and communicate security incident management processes, and oversee incident response, handling and escalation procedures.

1.8 Gather, analyze and utilize threat intelligence information.

1.9 Examine and make recommendations in the areas of cybersecurity in the organization, in a step to be reviewed and approved by the delegate of board authority.

1.10 Measure the performance of the cybersecurity program, and measure the defined key risk indicators.

1.11 Develop measuring and monitoring process for the compliance with cybersecurity policy, standards and procedures.

1.12 Develop and conduct cybersecurity awareness programs, and periodically measure the programs' effectiveness.

1.13 Periodically or on as-needed basis update board of directors and the committee about the status of cybersecurity program and initiatives.

2. Based on the size of the entity, cybersecurity responsibilities (not accountability) can be assigned to different – but dedicated – functional units positioned properly in the organizational structure.
3. The entity must establish an accountable management role with at least executive-level privileges to be accountable for cybersecurity function with adequate authority, reporting to the board of directors through the shortest path, and with no intersect with other conflicting positions. The position of the accountable person has to be:

3.1 Occupied by Jordanian.

3.2 Full-time appointment.

3.3 Qualified, in terms of:

- 10 years of experience in a related IT field of which 5 years in the Information/Cyber Security domain.
- A Bachelor degree in a related major as a minimum.
- Maintaining at least one active certificate of the Information Security Management international certifications such as CISSP, CISM, ISO 27001 Lead Implementer.

IT Management

In the context of cybersecurity, IT management is responsible for:

1. Implementing policies, controls, standards and guidelines emanating from cybersecurity program over systems and services.

2. Committing to acceptable risk levels and limits, and informing Information Security Management about any raised risks, gaps, and breaches related to approved and acceptable risk limits and levels, or any policy violation.
3. Remediating security vulnerabilities in timeframes according to their criticalities.
4. Maintaining and monitoring security tools and technologies. This includes regular update and maintenance for the applied security measures.
5. Committing to security incident response program, and maintaining a well-defined and documented plan of actions to put into place if a security incident does occur.

Executive Management, Business Process Owners and others

1. Executive management, business owners and relevant departments are responsible for reviewing cybersecurity assessment results. They have to ensure results are within approved risk ratios, and appropriate and timely corrective actions are taken for handling of reported assessment findings and gaps to keep the organization within cyber risk appetite.
2. Employees at all levels, internal departments and organization units, and external third party service providers are responsible for being in compliance with the cybersecurity policy, standards, and procedures.

A.2. Cybersecurity Strategy and Policy

Cybersecurity strategy

To define and implement the cybersecurity strategy, the entity needs to:

1. Define the desired cybersecurity state and objectives in alignment with:
   1.1 Business strategic goals and business objectives.
   1.2 Stated risk appetite and risk assessment process outputs.
   1.3 Regulatory and legal compliance and business process requirements.
   1.4 Sectoral cybersecurity strategy and initiatives.
2. Clearly determine the current state of cybersecurity based on currently deployed technical and procedural controls, as well as current cyber risks, threats and vulnerabilities.
3. Perform a gap analysis comparing between the current state and the desired state, and develop the road map that embeds prioritized initiatives and projects to achieve defined cybersecurity objectives, monitoring key performance indicators and reporting paths.
4. Develop a cybersecurity program to implement the strategy and identify accountability and responsibilities of implementing and monitoring the strategy.
5. Approve the strategy by the board of directors.
6. Set annual and change-driven review for the strategy.

Cybersecurity policy

The entity has to define and develop the cybersecurity policy that:

1. Clearly aligned with strategic cybersecurity objectives and includes high-level statements of management intent, expectations and directions based on national and international best practices, frameworks and standards, and supported by detailed standards, procedures and guidelines.
2. The policy should define cybersecurity objectives and scope, senior management commitment, cybersecurity roles and responsibilities, enforcement means and deterrent controls, and should address at least:
   2.1 Classification of information assets based on the criticality and sensitivity.
   2.2 Protection of information assets and data.
   2.3 IT operations, processes and related procedures, as well as the use of technologies and services.
   2.4 Application development and system acquisition.
   2.5 Embedding cybersecurity in business continuity management and plans.
   2.6 Management and handling of cyber and information incidents and data breaches.
   2.7 Human resources security, as well as awareness at all levels of the organization.

2.8 Compliance with legal and regulatory requirements, in addition to meeting contractual obligations.

2.9 External vendors, contractors, service providers and third parties cyber risk management

2.10 Physical security.

3. Approved by the board of directors.
4. Expected to remain fairly static for extended periods and to be considered as an input for other corporate policies (e.g. human resource policy, internet usage policy, etc.).
5. Well communicated with relevant stakeholders.
6. Reviewed at least annually or after major changes on business processes or business environment, or when new regulatory requirements are mandated.

B. Cyber Risk Management

B.1. Cyber Risk Management Process

1. Cyber risk appetite and risk tolerance statement must be defined, and approved by board of directors. Determining cyber risk appetite and tolerance values and thresholds depends mainly on the adopted and deployed methodology.
2. The entity has to develop, define and implement cyber risk management process aligned with enterprise risk management process to protect the CIA of identified information assets in a manner that achieves a balance between realizing opportunities of gain, and minimizing vulnerabilities and loss.
3. The cyber risk management process must be approved by the board of directors or the delegated committee.
4. Cyber risk management process has to:
   4.1 Address cyber risk identification, analysis, evaluation, treatment, review and monitoring processes.
   4.2 Specify involved parties, as well as risk owners. Involved parties should include business owners and IT specialists. Assessment outputs must be reported to risk owners to accept considering the approved cyber risk appetite and tolerance statement.
5. Cyber risk management process must be initiated prior to the development of cybersecurity strategy, and then outcomes are monitored and reviewed. The assessment must be conducted once every two years or less based on the risk profile, prior to a change on business or technical environment, prior to contracting a vendor or a third party service provider, and at the beginning of a project.
6. The expected outcomes of the cyber risk management process are:
   6.1 Understanding of threats, vulnerabilities and risk profiles.
   6.2 Understanding of the priorities based on the potential consequences of compromise.
   6.3 Understanding of mitigation strategy and treatment plans.
7. Cyber risk management process must be documented and communicated with concerned stakeholders, and awareness programs about the process must be conducted.
8. Risk management framework should be built based on international best practices and standards such as **NIST, ISACA Guidelines (e.g. COBIT) and ISO**.

B.2. Cyber Risk Assessment

B.2.1. Information Classification

1. Information classification process must be conducted regularly, and considers the potential impact and cost of consequences resulting from losing information confidentiality.
2. Information must be classified based on enforced laws and regulations. Information should be classified at least into four categories in the context of public, internal use, secret and top secret.
3. Well communicated and continuously reviewed on both change and regular basis.

B.2.2. Assets Valuation and Activities Prioritization

1. Information assets must be categorized and prioritized based on the total values of assets.
2. Semi-quantitative approach can be deployed to express total value of asset.
3. Well communicated and continuously reviewed on both change and regular basis.

B.2.3. Risk Identification

For each identified information asset; real and potential threats are determined, and the vulnerabilities subject to those threats are examined.

Threat identification

1. For each information asset, the entity can develop assumptions of misuse cases and risk scenarios clarifying threat events, types and actors (internal and external) that target the CIA of the information asset. Sources of threats information may include:
   1.1 Threat modeling processes. Modeling approaches can be attack-centric, system-centric or asset-centric.
   1.2 Assessment and audit functions.
   1.3 History of previous incidents.
   1.4 Brainstorming with business owners and users.
   1.5 Publications and intelligence information.
   1.6 Media.
   1.7 Contractors, third party and insurance service providers.
   1.8 CERTs threat libraries
2. The entity should develop and maintain a threat catalogue, and consider the different types and categories of threats including cyber-related natural, operational, political-motivated, financial-motivated, and accidental threats, and either deliberate or unintentional.

3. The entity has to consider the threats of internal actors that already have authorized access to the information asset whether employees, contractors, or external actors. Available information about active APT groups with financial motivations or targeting financial industries should be analyzed to deduce what threats the information assets might be exposed to. Emerging threats due to utilizing new or emerging technologies also should be considered.
4. Identified threats must be rated.

Vulnerability identification

1. The entity has to identify and examine the technical and procedural vulnerabilities and weaknesses resulting from flaws or deficiencies in:
   1.1 Governance procedures.
   1.2 Business processes.
   1.3 Design, implementation, and configuration.
   1.4 Technologies and underlying infrastructure.
   1.5 Physical and operating environments.
   1.6 Human errors.
   1.7 Contractors, supply chains and third party service providers.
2. Identified vulnerabilities must be rated.
3. To identify technical vulnerabilities for software, hardware or network information assets, the entity can rely on international sources of information about known vulnerabilities and weaknesses such as **NIST/National Vulnerability Database (CVE), NIST/Common Weakness Enumeration (CWE) and OWASP**. Also, the entity can adopt the vulnerability scoring system CVSS 3.1 consistent with the type and the position of the information asset (e.g. Internet or public-facing, communicating with untrusted networks or parties, RDBMS, security system, etc.) to rate technical security vulnerabilities.

Risk register

Information assets and identified risks are organized and maintained in a centralized register (i.e. cyber risk register), which is considered as a part of the cyber risk profile.

B.3. Cyber Risk Analysis and Evaluation

1. Entity has to define and conduct risk analysis and evaluation process.
2. Risk register must be updated with existing controls that intend to protect each identified information asset from the identified threats that could exploit examined vulnerabilities.
3. Entity has to calculate the actual risk value for each identified risk.
4. Entity has to assign risk owner for each risk (who is accountable for accepting the risk based on the risk appetite, and owns the controls associated with the tolerable risks).
5. Risk analysis and evaluation should highlight potential treatment areas.

B.4. Cyber Risk Treatment

1. The entity has to ensure the treatment of all identified and evaluated inherent cyber risks by one of the treatment options, and they are:
   1.1 Avoid the risk by terminating the activity.
   This option is valid when there is impossibility of reengineering the activity to manage the risk to an acceptable level or the activity doesn't worth the risk.
   1.2 Transfer the risk.
   This option is valid when the likelihood or probability of occurrence of the risk is very low but the threat impact is very high. Risk transfer could be in form of insurance agreements, indemnity agreements and/or outsourcing to third-parties with clearly stated liability and responsibilities.
   1.3 Mitigate the risk. This option could be achieved by implementing:
   - Detective controls to trigger preventive controls. Preventive controls and countermeasures are designed to reduce the exposure of the vulnerabilities and the threat impacts, thereby reduce the risk.
   - Corrective controls that are designed to reduce threat impact.
   - Compensating and deterrent controls that are designed to reduce the likelihood of the risk.
   - Controls include contractual, procedural, business and technical processes.

   1.4 Accept the risk.
   This option is valid when the cost of mitigation is too high in proportion of the total asset value, or the total risk value is less than the threshold of risk appetite.
2. The entity should maintain a risk treatment plan that defines the risks and the actions to remediate.
3. After remediation, the entity has to ensure that residual and secondary risks are tolerated and within acceptable levels. These risks must be reported to the risk owners to identify if more mitigation controls are required.

B.5. Cyber Risk Monitoring and Review

1. The results and status of assessment process must be continuously monitored and regularly reported on to the board of directors.
2. The effectiveness of implemented mitigation controls must be reviewed and evaluated at least annually.
3. Information related to identified risks must be tracked due to ever-changing threats and their conditions for the organization and for the industry.
4. Emergent risks must be reported, in order to address any new threats, vulnerabilities, and risk changes. If necessary, the report should provide actions to maintain acceptable levels of risks.
5. The entity has to develop Key Risk Indicators (KRIs) to provide an early warning of increasing risk exposures and on possible areas that introduce risks. KRIs need to be quantifiable and aligned with the risk appetite.

B.6. Project Management

1. Cybersecurity must be integrated at every stage during the project lifecycle by determining cybersecurity requirements that ensure the protection of collected, stored and processed data or information.
2. Cybersecurity requirements can be addressed and determined through performing risk assessment, evaluation process and threat landscaping at the beginning of a project, as well as at the beginning of every project stage. Identified risks and adequate mitigation controls must be registered and reflected into a project-related risk register. Also, cyber residual risks have to be within tolerable levels before approving project Go Live.
3. Cybersecurity-related roles and responsibilities must be identified.
4. Review process should be conducted to track the risk register and controls implementation.

B.7. Cyber Risk Insurance

The entity has to arrange for having in place a cyber risk or liability insurance coverage from an independent insurer, and based on the outcomes of the cyber risk assessment process. Insurance policy would at least include:

1. Expenses that are directly related to the first-party due to managing a crisis or an incident such as costs of forensic investigation, costs of breach notifications to customers and other affected parties, regulatory compliance costs, as well as monetary losses experienced by the crisis or the incident.
2. Claim expenses by third-parties such as costs of defending lawsuits and legal settlements, regulatory fines, and cyber extortion.

C. Cybersecurity Compliance

C.1. National Regulations and Standards

Entities have to ensure compliance with published cybersecurity-related and privacy-related instructions and circulations and what shall be published afterward by CBJ and national legislations, including but not limited to:

1. Cybersecurity Law no. (16) of (2019).
2. Electronic Transactions Law no. (15) of (2015).
3. Cyber Crimes Law no. (27) of (2015).
4. ByLaw of Electronic Payment and Money Transfer no. (111) of (2017).
5. Instructions on Cyber Risks Resiliency no. (26/1/1/1984) dated on (6 Feb 2018).
6. Instructions on Governance and Management of Information and Information Technology no. (65/2016) dated on (25 Oct 2016).
7. Instructions on Business Continuity Planning no. (27/2006) dated on (30 March 2006).

C.2. International Regulations and Standards

Entities should ensure the compliance with the latest versions of applicable international regulations and standards including but not limited to:

1. SWIFT CSP for SWIFT messaging infrastructure
2. PCI PTS for PIN entry card payment devices
3. PCI PA-DSS for developed card payment applications
4. PCI DSS for IT and operational environments of card payments
5. EMV technical standard

D. Cybersecurity Audit

D.1. Internal Audit

1. Cybersecurity audit process must be included within an audit program that is independent of any role that might conflict with the program in the entity, and mainly responsible for:
   1.1 Confirming the reliability of cyber risk identification process, assessing risk evaluation process and the risk is treated in line with evaluation process outputs across all business units.
   1.2 Verifying the implementation and completeness of the documentation process. Also verifying the comprehensive coverage of the developed policies, standards, procedures and guidelines, as well as confirming that formal approvals and enforcements are in place.
   1.3 Confirming the availability of mitigation controls and monitoring processes.
   1.4 Verifying incident management processes and evaluating incident response and handling procedures.
2. Cybersecurity audit execution plan must be approved by the board of directors or their delegates.
3. The board of directors and senior management, have to be briefed on regular basis or upon request about the assessments' findings and the progress of executing the audit plan.
4. Cybersecurity audit process should be conducted at least annually for high risk areas, once in two years for medium ranked risk areas, and once in three years for low ranked risk areas.

D.2. External Audit

1. Cybersecurity audit process must be included within the external audit program. The purpose of external cybersecurity auditing is to assure the comprehensiveness and the effectiveness of the cybersecurity program and the implementation of the program.
2. External cybersecurity audit process must be performed at least annually for critical and high business impact services, while other services can be scheduled on three years' audit plan.
3. The external auditor must be independent, qualified, and meet CBJ requirements.
4. The external auditors that are implementing external cybersecurity audit process must be changed every six years.
5. The board of directors and senior management, have to be updated on regular basis or upon request about the auditor findings.

E. Human Resources

E.1. Human Resources Security

The entity has to:

1. Conduct screening process prior to hiring new employees, temporary staff, promoted employees, and contractors that covers background verification and competence checks. Also, the process must be consistent with the applicable laws, regulations and ethics, and commensurate with the business requirements and the classification of the information to be accessed. The process should include validation and verification of at least:
   - Claimed identity
   - Criminal record
   - Financial credit history
   - Detailed qualifications
   - Previous employment history
   - Involvement in external businesses that could result in a conflict of interest
2. Conduct vetting process for all personnel on job periodically at least every five years. Vetting process should be consistent with the applicable laws, regulations and ethics, and include validation and verification of, at least:
   - Criminal record
   - Financial credit history
   - Involvement in external businesses that could result in a conflict of interest
3. Establish, enforce and maintain policy of acceptable use of information assets. The policy should include at least:
   3.1. Responsibilities regarding intellectual property ownership and copyrighted information.
   3.2. Conditions to grant access to classified information, as well as responsibilities regarding the classification, handling and transfer of information assets, either owned by the entity or received from external party.
   3.3. Responsibilities regarding user accounts and authenticators.
   3.4. Responsibilities regarding Internet and official email use.
   3.5. Responsibilities regarding clear screens and desks.
   3.6. Return of assets that should ensure the commitment of all employees, temporary staff and contractors to return assets upon termination. Non-return cases should trigger a security incident.
   3.7. Responsibilities regarding the reporting of observed suspicious activities.

3.8. Responsibilities regarding public declarations.

4. Clearly state terms and conditions in the contracts signed with employees, temporary staff and contractors to clarify information security general and individual responsibilities. Clauses should ensure overall compliance with cybersecurity policies and more specifically:
   - Acceptable use of information assets.
   - Obligations that remain valid after termination or change of employment.
   - Disciplinary actions on violations and security breaches.
5. Include Information Security roles and responsibilities in the job descriptions of related employees.
6. Review all granted physical and logical access rights to any personnel after changing role, and modify the rights based on new business needs.
7. Revoke all granted physical and logical access rights to any terminated personnel immediately. Physical and logical access rights must be disabled within maximum ninety days for inactive personnel.

E.2. Awareness and Training

A security awareness and training program must be established in which the entity has to:

1. Conduct regular awareness sessions – upon hire and at least annually – to address at least:
   1.1 Reinforcement of the compliance to the relative rules of cybersecurity policies and more specifically the documented rules of acceptable use of information assets.
   1.2 The importance of identification for any personnel (especially external personnel) claiming delivering maintenance service or asking for information.
   1.3 The importance of not installing, running and opening programs, emails and files from untrusted sources on both computer and mobile phone devices.
   1.4 The importance of not using the same credentials of the entity when registering for a service provided externally (such as learning websites).
   1.5 Observing suspicious behaviors, indicators and tampering around information, information assets and peripherals, as well as how to report observations and detected incidents.
   1.6 Cybersecurity threats in financial services industry.
   1.7 Consequences of abuse.
2. Conduct awareness sessions and programs aligned with the business context, and with orientation and segmentation based on the business roles of personnel and the levels of access.
3. Conduct dedicated awareness program for board members, senior and executive managers to ensure they have desired understanding of cybersecurity threats, vulnerabilities and controls relevant to their business roles, and their roles in developing the culture of cybersecurity.
4. Mandate personnel to acknowledge awareness and understanding of, and compliance with, relative cybersecurity policies at least annually.
5. Include temporary staff, contractors, suppliers and partners in awareness sessions or programs to ensure their understanding of their roles and responsibilities regarding cybersecurity.
6. Conduct awareness programs and campaigns for customers regularly to clarify potential cyber threats that target their interaction with delivered financial services, the recommended countermeasures and how to report incidents.
7. Deliver awareness sessions and programs through efficient channels. Channels could include classrooms, webinars, computer-based, social media, messaging and face to face conversations.
8. Conduct Specialized training programs for cybersecurity and IT staff. The programs should include training on cybersecurity-related products and services, as well as professional cybersecurity certifications based on roles of personnel and required level. The entity should mandate trainees to obtain and maintain relative certificates.

9. Conduct assessment process to measure the efficiency of awareness sessions and programs. Assessment process could include exams and launching social engineering simulated attacks (e.g. fake phishing emails or messages campaign, spoof identities over communication channels, etc.).
10. Continuous review, including mandatory training feedback mechanisms, for the contents of awareness and training sessions and programs.

PART2 Cybersecurity Technical and Operational Controls

F. Asset Identification

F.1. Identifying Information Assets

Data Storing and Processing Resources

1. Different types of resources must be inventoried. These resources include – but not limited to – containers, VMs, bare metals, storage systems (block, file and object), tape drives, client machines and VDIs. Dependencies among different types of resources should also be defined.
2. The inventory should include:
   2.1 Hosting sites and locations of resources for both on-premises and on-cloud.
   2.2 A unique asset-id assigned to each asset where applicable.
   2.3 Version of running platform or firmware.
   2.4 Model, part number and serial number of the asset where applicable.
   2.5 Asset ownership, ownership delegations, custodian and intended users. Ownership determines the responsibility of asset management during the lifecycle of the asset, and could be linked to individual, department or entity.
   2.6 The role and the position of the asset in the environment, and related business functions.
   2.7 Types of stored and processed data for each resource. Types of data can include core business data, PII, CHD, supportive business data, financial data, etc.
   2.8 Technical information about the resource (such as internal IP addresses, Internet access status, Internet or public-facing status and published IP addresses).
   2.9 End-of-life and end-of –support where applicable.
3. Well communicated and continuous review on both change and regular basis.

Software Assets

1. Commercial of-the-shelf, outsourced and in-house developed software, platforms and applications for both server-side and client-side must be inventoried.
2. The inventory should specify and contain:
   2.1. Hosting sites and locations of assets for both on-premises and on-cloud.
   2.2. A unique asset-id assigned to each asset where applicable.
   2.3. Container asset-id.
   2.4. Edition, version and built number
   2.5. Common Platform Enumeration (CPE) to the possible extent.
   2.6. Asset ownership, ownership delegations, custodian and intended users where applicable.
   2.7. Related business functions, and the role and the position in the environment in terms of:

- Production, development, test, etc.
- Hypervisor, OS, RDBMS, applications (business logic, access layer, middleware), etc.
- Delivering infrastructure service, management console, application portal, service-to-service API, mobile application API, etc.
- Client application or software, mobile application, etc.
- Underlying supportive firmware, software and programs.

2.8. Types of stored and processed data for each resource. Types of data can include core business data, PII, CHD, supportive business data, financial data, etc.

2.9. Technical information about the resource (such as internal IP addresses, Internet access status, Internet or public-facing status and published IP addresses).

2.10. End-of-life and end-of –support where applicable.

3. Aggregated lists could be maintained for widely installed software and programs.
4. Well communicated and continuous review on both change and regular basis.

Network Assets

1. Different types of resources must be inventoried. These resources include – but not limited to – Ethernet and SAN switches, routers, VPN concentrators, network-based security appliances and sensors and wireless access points.
2. The inventory should include:
   2.1 Hosting sites and locations of assets for both on-premises and on-cloud.
   2.2 A unique asset-id assigned to each asset as much as applicable.
   2.3 Model, part number and serial number of the asset where applicable.
   2.4 Version of running platform or firmware.
   2.5 Asset ownership, ownership delegations, custodian and intended users where applicable.
   2.6 The role and position in the environment, and related business functions where applicable.
   2.7 Technical information about the resource (such as management IP addresses, internal IP addresses, Internet access status, Internet or public-facing status and published IP addresses, serial numbers).
   2.8 End-of-life and end-of –support where applicable.
3. Well communicated and continuous review on both change and regular basis.

Network Segments and Communication Flows

1. Client-side, server-side, partner-side and published services side network segments and zones, as well as WiFi SSIDs and network segments must be defined.

2. The entity has to develop and maintain high-level and low-level network diagrams of the IT environment showing network segments, communication lines, network control points, and hosted and running services.
3. Data flows for critical and sensitive business processes either through digitized or not digitized channels must be defined and maintained. Data flows should include:
   3.1 Flows across internal and external systems, networks and trust boundaries.
   3.2 Processing and queuing systems, middleware, storing points, interconnections and entry points.
   3.3 Communication protocols and data types.
4. Well communicated and continuous review on both change and regular basis.

User-possession Devices and Media

1. Different types of user-possession devices and media must be inventoried. These types include but not limited to physical authenticators, external memory and storage means, tapes, cloud-based storage services.
2. The inventory should include:
   2.1 Owner, holder and/or custodian information.
   2.2 A unique asset-id assigned to each asset where applicable.
   2.3 Types of stored and processed data for each asset. Types of data can include authenticators, core business data, PII, supportive business data, financial data, etc.
3. Well communicated and continuous review on both change and regular basis.

Data and Information

1. Any collection of data that is processed, analyzed, interpreted, organized, classified or communicated in order to serve a business process should be inventoried (process to asset or asset to process). This includes information in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form.
2. The inventory should include owner, holder and/or custodian information.
3. Well communicated and continuous review on both change and regular basis.

IT Services and Processes

1. Delivered IT services must be catalogued and inventoried through having both service and technical catalogues.
   1.1 A unique asset-id assigned to each asset where applicable.
   1.2 Asset-ids of underlying data storing and processing resources and software assets.
   1.3 Service consumers where applicable.

2. Different IT operations and processes must be defined and maintained. These operations and processes should include at least:
   - Configuration management
   - Capacity management
   - Change management
   - Quality assurance and quality control
   - Backup management
   - Development
   - Operation and support.
3. For each listed IT service, operation and process; accountability and responsibilities shall be specified, as well as informing and escalation path through implementing a RACI model.
4. Well communicated and continuous review on both change and regular basis.

F.2. Identifying People

1. All employees at different levels, must be identified with their assigned roles and positions, as well as their competencies. Also, working and access hours (either physical or logical) must be identified.
2. Temporary staff, their assigned roles and working and access hours (either physical or logical) must be identified and logged.
3. Visitors, guests and staff of contractors and service providers, assigned projects or tasks, and working and access hours (either physical or logical) must be identified.
4. Continuous review for identification information on both change and regular basis.

F.3. Identifying Business Processes and Activities

1. The entity has to clearly identify and understand:
   - Business objectives and activities, as well as external stakeholders that influence the entity and are influenced by the entity.
   - Its role in the overall supply chain. Also, the entity has to understand its weight in the banking sector of Jordan.
2. Business processes must be inventoried. The inventory should include:
   2.1. Core and supportive business processes and related activities.
   2.2. Clarification of dependencies amongst different processes.
   2.3. Enabling IT assets for each business process.
   2.4. Well communicated and continuous review on both change and regular basis.

G. Prevention, Detection and Correctness

G.1. Physical Assets Security

G.1.1. Secure Access

The entity has to:

Areas and locations

1. Identify secure locations and areas that contain facilities to store, process or transmit sensitive and/or critical information. This could include – but not limited to – datacenters, offices and rooms, locations of access points and access network devices and telecommunication line paths.
2. Isolate logistic support areas such as loading, delivery and storage areas from identified secure locations and areas.
3. Define, approve and maintain list of authorized individuals to access secure locations and areas.
4. Protect secure locations and areas by physical and logical entry controls that only allow authorized personnel access based on business needs. Physical access control lists should be reviewed at least annually.
5. Avoid labeling hardware assets by clear references to roles, positions in the environment, and related business functions. The entity should keep hardware assets in secure areas and locations, rack mounted in lockable cabinets, and away from easy hand access where applicable.
6. Implement a procedure to:
   6.1. Distinguish amongst onsite personnel, temporary staff, visitors, and guests.
   6.2. Identify and authorize temporary staff, visitors and guests before entering secure locations and areas, and ensure that they are escorted all the time.
   6.3. Expire granted identification means to temporary staff, visitors and guests. Identification means must be collected before leaving the facility or when expired.

Assets off-premises

7. Mandate instructions to never leave assets off-premises unattended where applicable.
8. Consider and apply/implement technical and physical controls such as disk encryption, remote wipe and lock techniques where applicable.

Unattended assets

9. Lock any unattended or public-facing asset for the function that it was designed for only, as well as ensure no ability for unauthorized access to physical and logical components of the asset.
10. Put unattended assets in out-of-service mode after working hours (where applicable).

Clear desks

11. Establish clear desk policy and procedures. In certain areas where it may not be practical, a strong level of physical access control, and limiting number of visitors and external contractors shall be considered.
12. Establish a procedure to ensure not leaving valuable information presented on whiteboards, flipcharts and screens.

Data cables

13. Label data cables in a way that enables tracking from endpoints.
14. Protect data cables from interception and interference, and they are stretched in secure paths either underground or over ceiling.
15. Ensure that data cables that directly interconnect datacenter assets should not stretch outside the datacenter and secure areas.
16. Implement physical and/or logical controls to restrict access to publicly accessible network jacks.

G.1.2. Operation Physical Environment Protection

The entity has to:

1. Ensure the compliance with safety recommendations, guidelines and regulations for buildings/facilities codes. Environmental conditions and disturbances must be considered and integrated into the design and construction of the facilities including secure and critical mission areas.
2. Consider and implement applicable cybersecurity controls on all IT-enabled environmental controls and management systems.
3. Implement continuous monitoring, detection and protection controls for secure areas and critical missions' locations against environmental hazards including electrical power failures, temperature, humidity, and water leaks.
4. Establish, communicate, test and review evacuation plans.

G.1.3. Continuous Monitoring

The entity has to:

1. Maintain logs for accessing the facility and any identified secure areas or locations. The log should record:
   - Visitor names
   - Entry/leave times and dates
   - the firms represented
   - The onsite personnel authorizing the physical access.

   This must be applied for all temporary staff, visitors and guests. Retention of logs must be kept for at least six months.
2. Monitor access to secure areas and locations using video cameras and motion detection. Retention of recorded videos must align with local regulations.
3. Conduct preventive maintenance and regular testing procedure for monitoring equipment. Also, regular review for collected logs.

G.2. Resiliency by Design

G.2.1. Development, Test and Production Environments

1. The entity has to keep development, test and production environments separated at both, network and logical access levels, where:
   1.1 Separation is enforced with access control.
   1.2 No access for developers to production environment.
   1.3 Segregation of duties among the environments, and levels of authorization to move changes and artifacts from one environment to another, should be subject to the risk assessment outcomes.
2. Development environments must be protected and isolated in a way that at least:
   2.1 Restrict access to only authorized people and with controlled direct publishing over Internet if required only.
   2.2 Implement controls to ensure that no malicious or accidental development or update that may present security vulnerabilities.
   2.3 Strictly control the modifications to software packages or customization within a package to ensure no adverse impact on the internal integrity or the security of the application.
   2.4 Prohibit extracting data and source code from the environment.
   2.5 Ensure monitoring activity of developers either employees or temporary staff.

   This must be applied for development environments either on-premises or on-cloud (e.g. Cloud DevOps).
3. New developments and versions must be thoroughly tested in test environment. Prior to testing, test scenarios and criteria should be designed and developed based on business, operational and security requirements. The accountable manager of cybersecurity function and business owner should accept their respective test results.
4. In production environments, and based on risk assessment outcomes; the entity should implement one primary function per a computing instance.
5. Any test data and source code in a system must be removed before the system goes live in production environment. Only compiled code must be available on production systems.
6. The entity should not use production data for test or development purposes. Moving classified data and information outside a production container to another environment or onto local hard drives, removable media, and cloud storage must be prohibited unless explicitly authorized by the business owner and the accountable manager of cybersecurity function based on defined business needs, and taking into account anonymizing and masking data to the possible extent, as well as all related handling and secure deletion procedures.

7. The entity has to ensure that security level of the test environment is the same as production before moving any classified data and information.

G.2.2. Secure Development Lifecycle

1. The entity has to define and maintain a secure development lifecycle management process to ensure that security requirements are addressed during all phases of software development lifecycle or acquiring new software. Regardless of the adopted software development methodology, the process should consider:
   1.1 During the phase of requirements gathering, abuse cases as well as security and privacy requirements should be defined. Also, security risk assessment process should be conducted to identify the portions that require threat modeling and security design reviews.
   1.2 During the architecture and design phase, the entity should:
   - Ensure that defined security and privacy requirements are established.
   - Attack surface analysis and threat modeling processes are conducted to identify potential vulnerabilities and threats, as well as establishing appropriate mitigations.
   - Risk-based test scenarios and criteria are defined by a qualified quality control management function.

   1.3 During implementation and coding phase(s), developers have to consider adopted secure coding principles and practices, also static code analysis via code review should be conducted.
   1.4 During testing and verification phase(s), dynamic code analysis (via vulnerability scanning and penetration testing) must be conducted. Also, test cases and scenarios should be performed and the results must be reviewed and remediated.
   1.5 After release, the entity has to conduct defined security operations.
2. For critical acquired applications, the entity should arrange escrow agreements with the supplier to manage the source code.

G.2.3. Secure Coding

1. The entity has to establish and maintain a well communicated process to ensure that developers (either employees or temporary staff) of in-house applications shall:
   1.1 Consider security design principles over all development phases. The entity may adopt one of the international best practices (e.g. **OWASP Principles**). Any adopted practice shall consider the principles below at minimum:
   - Reduce attack surface and the risk of a successful attack. One approach to implement this principle is to limit potential vulnerable application functions to registered users only.
   - All available application security features should be enabled by default.
   - Implement fail-safe defaults by implying deny action for undefined behaviors and ensuring the application "fail" in a secure state.
   - Implement least privilege principle by granting minimum set of privileges required for the users to perform tasks as per their business roles.
   - Implement segregation of duties principle by assigning roles for each group of related application tasks, and ensuring the elimination of unjustified overlap among different roles.
   - Implement defense in depth principle by relying on multiple security controls to mitigate defined risks in different ways.
   - Validate every access attempt, as well as all data received, from third-party services assuming no trust or confidence is established.
   - Securing applications should not rely on obscuring core functionalities, source code, keys or strings.
   - Developing security controls should consider the use of simple and not sophisticated architecture and mechanisms. Also, it should not add difficulties to consume delivered application services.
   - For any detected security issue in an application, the root cause and other affected systems should be identified. Remediation must be tested thoroughly before releasing into production.

   1.2 Implement secure coding mechanisms and techniques. The entity can adopt one of the international best practices (e.g. **OWASP Secure Code Practices**). It is expected that any adopted practice shall provide countermeasures and address at least the risks, flaws and weaknesses defined in **OWASP Top Ten Web Application Security Risks and CWE/SANS TOP 25 Most Dangerous Software Errors**.
2. Based on the criticality and the sensitivity of the application, at least user activities (both privileged and regular), all access events (at network and at application levels) and any other security-related events

should be logged. Also, protection mechanisms for collected logs and audit trails against tampering, unauthorized access and deletion should be implemented.

3. All defined countermeasures against application threats must be implemented in all application portions and components, whether publicly accessible or restricted for registered users.
4. All secure coding requirements for in-house applications must be outlined in the agreements of supplying commercial off-the-shelf applications. The entity should ask for a certificate or evidence for commercial off-the-shelf applications to ensure security tests and vulnerabilities remediation are performed.
5. The entity has to conduct specialized training regularly for developers about the mechanisms and techniques of secure coding and avoiding common coding vulnerabilities.
6. Based on risk assessment outcomes, source code should be reviewed prior to releasing on production environment to ensure coding is aligned with adopted principles and practices, and to identify and remediate any discovered weaknesses. The review process should be conducted by individuals other than the coders. For outsourced code, independent review certification should be obtained.
7. Continuous review and monitoring for the established process.

G.2.4. Threat Modeling

1. For underdevelopment applications that process, transfer, and store critical and sensitive data and information, the entity should establish a managed and communicated process to perform threat modeling practice during the design phase, in order to identify potential vulnerabilities and threats, and to establish appropriate mitigation controls. The entity can adopt one of the international practices (e.g. STRIDE, PASTA, etc.). Any adopted practice should consider:
   1.1 Decomposing the architecture into fully detailed data flow diagrams that include:
      - Data processing containers and services such as compute instances, executables, static and dynamic libraries, etc.
      - Data stores such as files, databases, message queues, etc.
      - Data flows such as RPC calls, web API calls, web form calls, etc.
      - Actors, entry points and trust boundaries.
   1.2 Identifying and analyzing potential threats that might impact confidentiality, integrity, availability, authentication, authorization, accountability and non-repudiation security attributes of data and information during different processes, storage and transfer stages, as well as at the network, operating system, and application levels. Information sources about potential threats may include:
      - Brainstorming to define abuse cases and attack scenarios.
      - History of previous incidents.
      - Vendors, third party service providers and CERTs threat libraries.
      - Threat tactics, techniques and procedures that are addressed by global sources such as **OWASP Top Ten Web Application Security Risks, CWE/SANS TOP 25 Most Dangerous Software Errors, and MITRE ATT&CK Enterprise and Mobile Tactics and Techniques**.
      - Publications and intelligence information.
   1.3 Building a threat catalogue that defines:
      - Threat tactics (the technical goals) and related techniques (how to achieve the goals) for each identified threat.
      - Rating of each identified threat tactic and technique using one of the standardized risk assessment models and scoring systems (e.g. DREAD, CVSS, etc.)
      - Countermeasures for each identified threat tactic and technique.
2. The entity should define a procedure to ensure applying and implementing the outputs of the threat modeling process and the recommended countermeasures.
3. Continuous review and monitoring for the established process.

G.3. Identity Management, Authentication and Access Control

G.3.1. Identity Management

1. Identities must be verified, issued, managed, revoked, and audited for authorized individuals, devices, and processes. Dual-control mechanism should be implemented when registering new identities.
2. Identities must be proofed and bound to credential records and asserted in interactions. The entity should specify the desired identification assurance level for proofing identities by determining the acceptance proofing means and techniques. Identification process should not rely on self-asserted information.
3. Credential records must be maintained in secure repositories.
4. Identities must be verified before modifying any authenticators and credential record attributes.
5. To maintain accountability, deactivate all generic identifiers and limit shared identities among individuals by assigning unique identifier for each individual, and among devices and processes to the possible extent.
6. In case of using shared identities, a process must be performed to reissue the shared credentials when individuals are removed from the group.
7. The entity should avoid explicit association in naming convention between account addressing identifiers (e.g. email address, account number, etc.) and the real identifiers of the account owner (e.g. username) to the possible extent.
8. The entity should consider deceptive tactics to decoy high privileged accounts.
9. The entity has to separate between identity repositories and management systems used for accessing internal services, and the ones used for identifying outside customers for published and delivered services.
10. The entity can rely on external credential or trust service providers (outside the realm) for identifying external customers. The external credential service provider has to meet the identification assurance level defined by the entity.
11. For systems relying on external identity providers outside the realm, trust should be established using digital certificates issued from certificate authorities trusted by both parties wherever applicable.
12. Identities and credential records must be monitored to define abnormal behaviors and inactive identities.
13. Documented review of highly privileged accounts at least every 3 months, and documented review of normal user accounts at 6 months.
14. Identity management activities must be logged and monitored.

G.3.2. Authentication

1. Individuals, devices, and services have to be authenticated when requesting access to information assets and resources with authentication assurance level commensurate with the level of the risk that is associated to the access process.
2. The entity should consider the use of a centralized implementation of authentication services, with separate logic from the assets and resources being accessed.
3. The entity can rely on external identity providers (outside the realm) for authenticating external consumers. The external identity provider has to meet the authentication assurance level defined by the entity.
4. Authentication services and identity providers have to work based on the latest versions of standardized and robust authentication protocols (e.g. OAuth 2.0 with OpenID Connect 1.0, Kerberos v5, SAML 2.0, LDAPv3, RADIUS, etc.).
5. A trust relationship must be established with authentication services inside the realm and identity providers outside the realm (federated authentication). Trust with identity providers should be established using digital certificates issued from certificate authorities trusted by both parties wherever applicable, instead of using on pre-shared keys.
6. The entity has to separate between authentication services used for authenticating internal individuals and services, and the services for authenticating outside consumers of published and delivered services.
7. The entity has to consider authentication factors as below:
   7.1. Something You Know
      - Memorized secrets (e.g. password, PIN numbers, etc.)

   7.2. Something You Have
      - Out-of-band one use secrets, where the secret is sent by the entity through a channel and verified by the individual through another channel
      - Offline or online, time-based or hash-based OTP (hardware or software)
      - Cryptographic authenticator (hardware or software), where the individual is authenticating via proving the possession and control of a stored crypto key (i.e. private key).

   7.3. Something You Are
      - Physical biometric methods (i.e. fingerprint, face or iris recognition)

   7.4. Authentication can be considered multi-factor, if and only if, a combination of at least two authenticators of different factors is implemented to confirm the claimed identity. Other sets of combinations shall be considered as multi-step authentication.

   7.5. All implemented factors should be presented to the verifier (i.e. identity provider or authentication service). Factors used to protect the secret that will be presented to the verifier (e.g. PIN protecting

mobile-based OTP or hardware cryptographic authenticator) should not be considered as a second authentication factor.

7.6. Instrument/device verification, knowledge-based authentication, location data and behavioral biometrics cannot be considered as authentication factors. On the other hand, the entity should implement these factors as detective and preventive measures against credential and identity theft and spoofing attacks.

8. The entity has to establish, communicate and enforce password management policy and procedures. The entity has to ensure the enforcement and application of the policy, as well as monitoring the compliance either through automated or manual processes. The policy should address:

8.1 Password complexity, length, no reuse, expiry and minimum age to change, as well as account lockout thresholds, durations and unlocking procedure. These settings values can consider different risk levels associated to different identities assessed based on pre-defined criteria that may include – but not limited to –:

- The Criticality and sensitivity of information assets and resources to be accessed
- Privilege levels
- Number of implemented authentication factors
- The type the identities whether individual, service or device, as well as type of logon process, whether interactive or non-interactive.
- Crossing over untrusted boundaries
- Availability and adequacy of detective and preventive measures against credential and identity theft and spoofing attacks

8.2 Passwords and authentication keys must be encrypted and in irreversible encoded formats wherever stored and transferred.

8.3 Temporary and one-use passwords must be with short expiration, and sent to pre-registered addresses (e.g. mobile phone numbers, email addresses, etc.)

8.4 Individuals should be notified about last success or failed access, and last password reset.

8.5 Administrators can set a password for first-time use, and then enforce changing immediately after the first use. The administrator should avoid default and well-known passwords, or can rely on auto-generated random passwords.

8.6 Wherever possible individuals should be able to choose their own passwords.

8.7 Strong mechanisms should be applied for individual logons, such as mechanisms in the form of challenge-response authentication, and mechanisms in the form of encrypted form-based authentication (e.g. over a secure version of TLS).

9. Systems and applications should be designed to at least:

9.1. Provide a secure procedure to reset password.

9.2. Not store authentication data except on authentication services or identity providers, where passwords and authentication keys must be stored in encrypted and irreversible encoded formats.

9.3. Grant session IDs, tokens, or tickets for principles and services only after successfully authenticated.

9.4. Ensure randomness and unpredictability for generated session IDs, tokens, or tickets, and not re-using pre-generated ones.

9.5. Authenticate each access request with valid session ID, token, or ticket.

9.6. Secure stored session data at both client and server sides at least against tampering and hijacking.

9.7. Secure transfer of authentication and session data against tampering, unauthorized access and hijacking.

9.8. Monitor and limit concurrent logons for individuals.

9.9. Terminate inactive sessions after a specified period, based on the assessment of the criticality and the sensitivity of the system, application and exchanged transactions.

9.10. Destroy all session keys, granted session IDs, tokens, or tickets. Furthermore, session data must be destroyed from cache or memory trays in both client and server sides after expiration or logout.

9.11. For service-to-service communication that does not rely on an authentication service:

- Implement authentication on transport channels and exchanged transactions to the possible extent.
- If a service relies on a shared secret stored in a file or data store to authenticate, this secret must be kept encrypted asymmetrically, hashed, with access restricted to the intended service only. Also, auditing and alerting should be enabled for any failed access attempt.

10. The entity has to implement all facilities needed to at least:

- Log and review all (failed and success) attempts of authentication or access.
- Log changes to identification and authentication mechanisms for privileged and unprivileged identities, such as password change and identifier change.

G.3.3. Access Rights Management

The entity has to establish and maintain a well communicated process to manage access rights. The entity has to at least consider:

1. Defining access rights for each business role by determining information assets and/or resources and level of privilege required for access.
2. Provisioning access rights to individuals must require business justification and documented authorization from the information asset or resource owner.
3. For delivered services whether on premises or on cloud; the access of authenticated individuals must be restricted only to data which they own and are permitted to access, and the entity has to ensure the nonexistence of vulnerabilities that may enable unauthorized access even within the restricted parts of the system or the application.
4. Restrict access based on least privileges, permissions required for performing the needed routine operations and responsibilities of the business role.
5. Additional required privileges (elevations) and permissions must be at least:
    - Justified and verified based on the requester role and competencies.
    - Tightly controlled to avoid affecting the CIA of the accessed information asset or resource.
    - Granted on a temporary basis – to the possible extent – after being authorized by the information asset or resource owner.
    - Documented and logged.
6. Third party, temporary staff, contractors, outsourced staff and vendor individuals logical access must be granted on a temporary basis and time limited to actual business needs, as well as recorded and monitored to the possible extent.
7. For highly classified critical and sensitive business activities and IT operations, duties and permissions should be divided between at least two different individuals from different groups, to ensure these activities or operations are not performed by the same individual (i.e. dual control), as well as to ensure the inability to bypass dual control.
8. Multifactor authentication must be enabled in critical and sensitive systems for permanently and temporarily assigned privileged roles.
9. A process for immediately reporting any exceptional granted access rights should be defined. The process should ensure checking granted rights against the pre-approved authorization rules.
10. Granted access rights to individuals must be regularly reviewed, modified on role change basis and revoked upon termination.

11. Authorizations for privileged access rights must be frequently reviewed by the owners of information assets and resources.

G.3.4. Logical Access

Network and network services access

1. The network (i.e. access points, access network switches, and VPN gateways) has to authenticate and authorize (such as assign network segment) each device and individual before starting data transmission. Authenticating devices should rely on cryptographic operations that do not rely on pre-shared keys.
2. Moving across network segments and accessing network services (e.g. Internet) must be restricted with access control at network level (e.g. stateful or application-layer firewall) that implies deny action unless explicitly permitted.
3. Permitting access to the network and network services at the network layer should be identity-based, and integrated with the identity management system.
4. Documented review of network access rules at least every 6 months.

Infrastructure access

5. Individual interactive logons should be restricted to specific physical or virtual endpoints based on business needs, and should not be granted to logon as a service and as a batch, as well as network access to information assets and resources unless explicitly authorized.
6. Interactive and remote logon to infrastructure components and compute instances with privileged accounts should be avoided to the possible extent. Logon should be performed through normal individual accounts with the ability to escalate to administrative privileges using different and privileged account credentials (e.g. runas and sudo).
7. Interactive logon with super accounts (e.g. root and administrator) should consider:
    - Restriction only to logon into maintenance mode, during emergency cases, and to perform installation and configuration tasks.
    - Sessions should be terminated immediately after completing the task.
    - Passwords should be changed after completing the task
    - Logon with privileged accounts should be documented
8. Restrict individual ability to download and install programs that might override infrastructure and operating systems controls. Use of such programs must be managed, monitored and logged.

Application access

9. Access to information, all application system components, functions, and extracting information must be controlled based on the business role and privilege level of the individual. Applications have to imply deny default actions. The entity has to ensure that no vulnerabilities existing which may enable unauthorized access even within the restricted parts of the system or the application.
10. All individual access except database administrators to data in RDBMS should be restricted through programmatic methods.
11. Application access to data in RDBMS should rely on identities not used by individuals or services.
12. Rights and permissions for application services at the level of infrastructure and operating system levels should be tuned to avoid granting permanent privileged rights and permissions.
13. Established password management policy should consider application and service identities.

Administrations and management access

14. For administration purposes, the entity should adopt an infrastructure access control model that minimizes the risk of escalation of privilege by restricting the controls of administrators, as well as where administrators can interactively logon and access information assets. This could be achieved by:
    - Dividing IT infrastructure servers and services amongst different security tiers.
    - Administrators of higher tier can control lower level information assets but cannot logon into, on the other hand, administrators of lower level cannot control higher level information assets.
    - The highest security tier should include identity management services, where lowest security tier should include endpoints.
15. Highly privileged IT administration rights and permissions should not be delegated.
16. Non-console administrative access must be encrypted.
17. Managing network and security infrastructure components should be via dedicated management interfaces (i.e. out-of-band management interface) accessed through a controlled network (e.g. management VLAN).
18. Authentication services for identities used to manage network and security infrastructure components must be separated from the identities used to access other infrastructure components, systems and applications.
19. Privileged business tasks, IT operations, and administrative tasks should be implemented through physical or virtual workstations that are located in logical secure zones and locked to the intended tasks. Workstations should not have access to potentially threat-exposed points (e.g. Internet, email services, remote access, etc.) to avoid identity attacks, leaking credentials, being part of lateral movement paths and being points of maintaining covert channels.

20. The entity should implement granular control of infrastructure components, servers and compute instances through creating different jump servers. Each should be mapped to and located on one server-side security zone where administrators can access managed servers through the jump servers.
21. Administrative and management tasks should be performed using management tools instead of interactive or remote logon into managed servers and compute instances.
22. All actions taken by privileged accounts on infrastructure components and servers must be logged and sessions should be recorded.

G.3.5. Network Segmentation and Zoning

1. Server-side compute instances (i.e. physical machines, VMs, containers, etc.) either on premises or on cloud must be located in different layer 2 or virtual cloud network segments based on the running system and its role. For a single system, each tier (e.g. access, business logic and RDBMS or data store) should be located in different segment.
2. Data traffic segments should be separated from control traffic segments (e.g. cluster heartbeats, replication, management, etc.)
3. Network zones that have similar requirements of data and information protection can be considered as a secure zone. If there is no business need, trust relationships between identity and authentication services that are located in and serving different fully isolated secure zones should be limited.
4. Network segmentation can be achieved physically or logically (e.g. VLANs). The entity should consider implementing physical security and IT-enabled environmental control and management systems over physically separated networks and locations.
5. Wired and wireless client-side networks must be segmented and zoned based on business roles and level of privileges granted.
6. Separation amongst network segments must be enforced with access control at network layer that explicitly permit traffic based on the application recognized or at least layer 4 information.
7. All actions taken on network segments and zones must be logged and monitored.

G.4. Data Protection

G.4.1. Data Confidentiality

1. Confidentiality of classified data and information in all formats must be protected at rest by at least considering:
   - Implementation of encryption mechanisms on content, file, application, operating system, and/or storage levels.
   - Restricting physical and logical access to only authorized individuals, services, and devices.
   - Limiting storage points and replicas of classified data and information.
   - Moving classified data and information outside the custodian container must be prohibited unless explicitly authorized by the business owner based on defined business needs, anonymizing and masking data to the possible extent, as well as implementing protection measures and procedures that ensure no disclosure of confidentiality outside custodian containers.
2. Confidentiality of classified data and information in all formats must be protected during transmission by considering the implementation of encryption and access restriction mechanisms at transport channel and/or at transmitted content levels.
3. The entity has to anonymize, tokenize and/or truncate any classified data and information sent over out-of-control untrusted transport channels (e.g. GSM). Complete send of classified data and information over such channels should be limited to temporary and one-use passwords with short expiration.
4. Transmitting classified data and information over physical transport media (e.g. mail) has to use tamper-evident sealed package.

G.4.2. Data Integrity

Integrity of information and data must be protected by at least considering:

1. Information and data integrity must be protected at rest, and should consider at least the following:
   - Classified user data and information
   - Operating system files and boot sectors
   - Running software and application executables and static files (for content modification and unexpected file addition or deletion).
   - Databases records (not data or log files). Full referential check on all records should be performed.
   - Existing systems and applications logs and audit trails
   - Continuality and regularity of performing integrity check processes should depend on the risk assessed, as well as the classification of the information assets.
2. The source and integrity of software, security updates and patches must be checked and validated before installing or applying.
3. Integrity check for information or data at rest may rely on verifying the source-provided checksums and digital signatures where applicable. Protecting the confidentiality of data and information should also be considered in order to protect the integrity wherever applicable.
4. Critical and sensitive information assets should be configured to run and execute only trusted software. This can be accomplished by utilizing whitelisting techniques.
5. Integrity check processes must ensure detecting and logging or alerting for any file changes or unexpected additions. Alerts should be considered as forensic data.
6. Systems and applications have to ensure data and information integrity during transmission, and should consider at least:
   - To depend on digital signing rather than checksums to validate the integrity, as well as applying confidentiality controls at transport channel and/or content levels.
   - To timestamp transmitted messages and/or to embed nonce to avoid replay attacks.
   - Sequencing transmitted messages in a way that enables the detection of incorrectly sequenced transmissions (i.e. out-of-orders).
   - Referencing the dependencies of transmitted messages.
   - Detecting and handling duplications.
   - Transmitted messages should be acknowledged to ensure proof of delivery.
   - Network layer of the transport channel should rely on TCP protocol, and hardware should use ECC RAM.

7. The integrity check can be a manual process, integrated into the product, or can rely on a third-party tool.

G.4.3. Authenticity

For business-impacting data and transactions, applications and systems should implement mechanisms to ensure that received data is authenticated, and that is generated from a genuine source in a way that protects from man-in-the-middle attacks (e.g. end-to-end mutual TLS authentication):

1. In case of using a mechanism that relies on symmetric cryptographic (e.g. HMAC), then shared secrets must be protected securely to prevent unauthorized access and disclosure.
2. In case of using a mechanism that relies on asymmetric cryptographic (e.g. Digital Signing and certificate-based authentication), then private keys must be protected securely to prevent unauthorized access and disclosure. With third-parties and services outside the realm, public keys should be in a form of X.509v3 digital certificates issued* from a trusted CA.

G.4.4. Repudiation

For business-impacting transactions, the entity should consider implementing mechanisms to ensure that the initiators of transactions are provided with proof of delivery, and the recipients are provided with proof of the initiators' identity, so neither can later deny having processed the information. Digital signing is one of the accepted mechanisms to achieve non-repudiation. Implemented digital signing mechanism has to fulfill the legal requirements articled in **Electronic Transactions Law no. (15) of (2015)** in order to be acknowledged by Jordanian courts.

G.4.5. Data Privacy

1. The entity has to develop, maintain, implement, and communicate a data privacy policy. The policy and procedures should address and include the following:
   1.1 Personal data is processed lawfully, fairly, and in a transparent manner to the data subject. Lawfulness of collection and processing personal data should be based on:
   - obtaining a clear, explicit and undeniable consent of the data subject,
   - contractual obligations where the data subject is party in the contract, or in order to take specific steps requested by the data subject prior to entering into a contract,
   - legal obligations where the entity is subject to,
   - an official function or a task in the public interest, and the function or the task has a clear basis in law or regulations.
   - legitimate interests pursued by the entity or a third-party unless these interests are not overridden by the interests or fundamental rights of the data subject which require protection of personal data.

   1.2 Data subject should have the ability to define expiry of the consent, as well as the right to withdraw the consent at any time.
   1.3 Personal data is gathered on an as-needed basis for predefined, explicit and legitimate purposes. In addition, data is relevant and limited only to these purposes.
   1.4 Personal data is stored and processed in a way that identifies data subject for no longer than what is needed for the predefined purposes. Archiving personal data has to fulfill the legal and regulatory requirements.
   1.5 Data subjects should have the right to personal data erasure after withdrawing consent, or the data is no longer needed for the original purpose for which the data was gathered, unless required by legal or regulatory requirements.
   1.6 Ensuring data security (confidentiality and integrity) during transmission, processing, and storage.
   1.7 Ensuring data quality through maintaining data cleansing and updating processes to correct any inaccurate data.
2. The policy must be communicated with third parties, service providers, and vendors, and the entity has to ensure the compliance of these parties with the policy.

G.4.6. Data Leak

1. The entity has to develop, maintain, implement and communicate data leak detection and prevention procedures that:
   1.1 Clearly define all points through which classified data and information could be leaked intentionally or unintentionally. Scope of potential leakage points may include:
   - The level of endpoints and hosts such as USB flash memory, CD/DVD, etc.
   - The level of intranet, extranet and internet-facing application and network services such as copying, printing, email, HTTP/S, SQL, SMB, FTP, SCP, etc.
   - Located on both on-premises and on-cloud.
   - Physical such as papers.

   1.2 In addition to ensuring data security during transmission, processing and storage, the entity has to control potential leakage points by applying data and information leakage detection, alerting and prevention controls. It's expected that such controls and tools can detect and prevent transfers:
   - Of data and information through the potential leakage points based on predefined classification rules.
   - Via either plaintext or encrypted formats with fail safe defaults by implying deny action for un-interpreted contents.
2. In the event of a breach affecting classified business data and/or information (e.g. personal data, employee records, financial data, etc.), the entity has to at least:
   - Clearly define the scope of the breach (i.e. affected data subjects and breached data attributes)
   - Conduct impact assessment process to define containment controls and estimate the cost of consequences.
   - Immediately communicate with affected data subjects where that breach is likely to result in a high risk in order for them to take necessary precautions.
3. In the event of a breach affecting classified technical data and information (e.g. source code, credentials, internal network designs and data flows, etc.), the entity has to at least:
   - Clearly define the affected systems and applications.
   - Ensure patching all known vulnerabilities and conduct new vulnerability scans.
   - Ensure having no hard coded credentials. If there is a technical limitation, change all hard coded credentials, passwords and authentication keys immediately. Hard coded credentials, passwords and authentication keys should be encrypted and in irreversible encoded formats wherever stored and transferred.
   - Conduct impact assessment process to define containment controls and cost of consequences.

4. The entity has to communicate with contractors, outsourced service providers and third parties that are custodians and processors for classified data and information to ensure their adherence to the implemented procedures.

G.4.7. Email Security

1. The entity has to develop, maintain, implement and communicate email usage policy and procedures that should include:
   1.1 Controlling email service access and use based on clearly defined and managed access rights granted on a business need basis.
   1.2 Acceptable use of email service.
   1.3 Guidelines of detecting phishing emails and spam, safe handling for attachments and links, and safe sending, forwarding and replying.
   1.4 Adherence to data security and data privacy requirements. Also, this must be communicated with contractors, outsourced service providers and third parties.
   1.5 Users should be provided with any needed tools and mechanisms (e.g. S/MIME) to digitally sign/verify and encrypt/decrypt individual emails that contain highly classified and business-impacting data and information.
   1.6 Appending disclaimers to warn that a confidential content may be forwarded.
2. The entity has to implement controls to at least:
   2.1 Prevent the mail service from being "open relay" by specifying trusted domains or IP addresses from which to relay emails.
   2.2 Screen the content of circulated/nested emails to detect malicious attachments and embedded links.
   2.3 Protect against spam emails and emails with blacklisted senders, domains and IP addresses.
   2.4 Detect and prevent classified data and information leaks.
   2.5 Ensure the authenticity of the received emails on boundaries via at least:
      - Maintaining PTR records for the owned public IP addresses that initiate SMTP sessions. These records should refer to the domains and hostnames exist in the sent EHLO/HELO messages. Also, the entity has to apply reverse DNS lookup for unauthenticated incoming sessions.
      - Maintaining an SPF record under its authoritative DNS referring to only the IP addresses or subnets that are authorized to send email on its behalf. Also, the entity has to apply mechanism to validate and check SPF record for incoming emails.
      - Applying DKIM security standard to digitally sign bodies and headers of sent emails, as well as maintain DKIM record(s) under the authoritative DNS. Also, the entity has to apply mechanisms to validate DKIM signature header for incoming emails.
      - Maintaining DMARC policy record under the root level of the authoritative DNS. In the policy record, the entity should specify:
        – Initially "none" action for non-aligned emails under the domain and all subdomains belonging to the entity.

– Two email addresses, one to receive aggregate DMARC reports and another to receive forensic DMARC reports. Copies of forensic DMARC reports must be forwarded to int.fincert@cbj.gov.jo.

Also, each entity has to apply mechanisms to check DMARC of incoming emails based on validating both SPF and DKIM.

- The entity should authenticate SMTP sessions with trusted parties using TLS to the possible extent.

3. Apply an email retention policy in accordance with data retention and data privacy policies.

G.4.8. Removable Media

1. The entity has to develop, maintain, implement and communicate removable media usage policy and procedures that should include:
   1.1 By default, the usage of external storage media at endpoint and server levels should be blocked and prohibited unless explicitly permitted and approved by information security management based on justified business needs. Use-specific risk should be assessed when excepting business/IT administration or operation, or a machine used by customer-facing employee. Granted permissions and exceptions must be logged.
   1.2 The content of any re-usable media should be made unrecoverable and securely destroyed once finishing the purpose of use.
   1.3 For backup media and media storing classified data and information, encryption mechanisms must be deployed and the media must be stored in a physically secured location.
   1.4 Security inspection in an isolated environment for removable media that is received from outside before starting any processing of its content.
2. Transferring media that contain classified data and information must be protected against unauthorized access or corruption during transportation. Protection should consider the reliability of the transport, packaging in order to protect against physical damage, and logging of the transferred content and protection measures applied should be kept.
3. For media no longer needed, a documented procedure must be followed for disposing. The procedure has to ensure minimal risk of confidential information leakage.

G.5. Information Protection

G.5.1. Configuration Management

The entity has to develop, maintain, implement and communicate configuration management policy and procedures to ensure maintaining configuration items in a desired and consistent state. The defined policy and procedures should consider controlling initializing, changing, and monitoring the configurations.

1. Identify each part of each system (i.e. configuration items) that is a discrete target of configuration management processes (e.g., hardware, hypervisor, OS, application software, security software, network appliance, documentation, etc.). This step should be achieved through the process of asset inventory.
2. Define baseline configuration via defining set of specifications for each system and each configuration item within a system. The baseline for a given point of time should be formally reviewed and agreed on. All changes to be processed through a change management process. The baseline should at least address:
    - Configuration settings
    - Software loads and patch levels
    - How the information system is physically or logically arranged.
    - How various security controls are implemented.
    - Documentation procedure.
3. Define monitoring process for assessing the level of compliance with the established baseline configuration. Also, the entity should deploy the mechanisms for reporting on the configuration status of items placed under configuration management.

G.5.2. Change Management

The entity has to develop, maintain, implement and communicate change management policy and procedures to ensure considering defined security controls in the complete cycle of the change management.

1. Defining handling procedures for different types of changes:
   - Pre-authorized standard changes that follow predefined procedure.
   - Emergency changes that need to be implemented immediately.
   - Normal changes.
2. Assigning a change manager as an owner of the change management process, as well as establishing a Change Advisory Board (CAB).
   2.1. Change manager is responsible for finally approving specific change categories, prioritize changes, and tracking and monitoring status of changes.
   2.2. CAB is responsible for estimating impact, required resources, finally approve or review/confirm change manager approvals, and schedule changes based on the priority. Members of CAB may at least include:
      - The accountable manager of cybersecurity function
      - Heads of IT administration and operation staff
      - Business owners
      - Customer relationship managers and service desk agents
3. Normal changes should be classified by the change manager into at least three categories, major, significant, and minor, based on the complexity and the level of risk involved. Each category requires different change authorities:
   3.1 Request for changes should be initially approved by business owners and then the accountable manager of cybersecurity function before submitting to change manager.
   3.2 Major and significant changes have to be submitted through change manager to CAB for final approval after initially defining the risk of consequences and needed mitigation measures.
   3.3 Minor changes can be finally approved by change manager. Approvals should be reviewed/confirmed by CAB to allocate resources and schedule the change.
   3.4 For emergency changes, change manager can contact directly with the senior management, cybersecurity committee or board of directors.
4. Define and execute test and back-out plans for each approved change. Test plans must be executed in the test environment and should consider:
   - Functional and user acceptance test, integration test, and stress test.

- Security tests include identity management, exception handling, logging and auditing functionalities, static code review to the possible extent, and dynamic code analysis through vulnerability scanning and penetration testing.

5. Appropriate documentation, testing and approvals should be in place before implementing the change in production environment.
6. Implementation results must be logged and monitored.
7. Post-implementation review for cybersecurity controls (configuration, asset inventories, etc.), and measuring the effectiveness of the infrastructure and network cybersecurity controls.
8. The compliance with change management policy and procedures should be monitored.

G.5.3. Patch and Vulnerability Management

The entity has to develop, maintain, implement and communicate application and infrastructure vulnerability management policy and procedures to ensure timely identification and effective treatment of vulnerabilities.

1. Scoped assets in the vulnerability management policy and procedures should include all identified configuration items such as:
   - Hypervisor, Operating systems, firmware and drivers
   - Server, desktop and mobile applications, as well as middleware and RDBMS
   - Network Appliances
2. Methodologies of identifying vulnerabilities should include at least:
   2.1 A periodic process to correlate and find matches between inventoried CPEs, published CVEs and related CVSSs.
   2.2 Receiving advisories from vendors, external partners and CERTs through trusted channels such as emails, vendor or service provider portals, and patching management software.
   2.3 Findings of vulnerability scanning and penetration testing processes, as well as other cybersecurity controls.
3. Possible corrective controls should be defined based on CVE and vendor recommendations. The corrective control may negatively affect business application(s) and processes. In such case, compensating controls should be defined, and if this is not applicable, a risk assessment process should be conducted.
4. Treatment should go through the approved change management process. Categorizing and prioritizing vulnerabilities should consider:
   - CVSS score value, the exposure level to a threat event, and whether the vulnerability has been exploited before.
   - The type and the position of the vulnerable asset (e.g. Internet or public-facing, communicating with untrusted networks or parties, RDBMS, security system, etc.).
   - The weight of the vulnerable asset based on the criticality and sensitivity.

G.5.4. Capacity and Performance Management

The entity has to develop, maintain, implement and communicate capacity management process to ensure that IT resources are correctly sized to meet current and future business needs (in cost-effective and business-driven manners). Capacity management process should ensure that:

1. Required service levels for business plans should be specified based on business criticality. Sizing process based on realistic assumptions should be conducted to determine IT resources (i.e. computing resources, networking resources and storage resources) required over a period of time. The period of time should be aligned with the lifetime of underlying IT assets. Business plans are then translated into IT services, architectures and resources.
2. Continuous monitoring, measuring and analysis for end-to-end service delivery and asset-level performance such as loads, throughputs, latencies, storage utilization, as well as downtimes and causes of reported service unavailability cases.
3. Thresholds for capacity monitoring processes should be predefined and considered for triggering a process to provide IT resources as needed.

G.5.5. Backup and Restoration Management

The entity has to develop, maintain, implement and communicate backup management policy to identify the procedures and actions needed to manage data backup processes.

1. The policy should clearly at least address:
   1.1 What data to be backed up considering business criticality.
   1.2 Backup periodicity.
   1.3 Backup and restoration management, storage and media solutions and technologies.
   1.4 Security measures to protect backed up data CIA.
   1.5 Monitoring backup and conducting periodic restoration tests.
2. The entity has to have offsite location for storing data backups with absolutely no accessibility over the in-band network.

G.5.6. Data Retention and Destruction

The entity has to develop, maintain, implement and communicate data retention and securely destruction policy and procedures to ensure protection against leakage and unauthorized access when disposed.

1. Retention and archiving of information assets should be defined in accordance with legal and regulatory requirements, as well as business needs.
2. The entity has to ensure that storage media will not degrade during the required storage period.
3. Information assets should be disposed and destroyed when no longer needed in accordance with legal and regulatory requirements, by using techniques and permanent erasure means to make the recovery of classified data and information impossible.
4. The entity should ensure implementing the data retention and destruction policy when data is processed and/or stored by third parties, service providers and vendors according to data classification.
5. The entity should ensure cloud service providers adherence when data and information are no longer needed or when transferred out (i.e. exit). The entity can clearly state this cloud service provider's obligation in the contract.

G.6. Infrastructure and Network Security

G.6.1. Protection Technologies

1. The entity has to enforce access control amongst network segments by deploying network firewall functionality. The firewall should be:
   1.1 Able to recognize the applications of the passing traffic.
   1.2 Restricting access by explicitly permitting only required applications.
   1.3 Granting user access based on the identity where applicable.
   1.4 Maintaining state of network connections to permit only established ones.
   1.5 Protecting against source IP spoofing.
   1.6 Protecting against anomalous traffic.
   1.7 Able to inspect encrypted flows to recognize and control passing traffic and applications.
   In addition, network firewall functionality must be applied for incoming traffic from wireless networks to the enterprise network. Permissions must be granted explicitly and only to the authorized traffic based on the business needs.
2. The network should be configured to prevent private IP addresses and routing information disclosure to unauthorized parties.
3. For publically accessible services, implement DMZ(s) segregated from trusted network zones, and limit inbound traffic to specified IP addresses, protocols, and ports, as well as applications where applicable.
4. Application-layer firewall shall be deployed, in order to protect published web (both application and API) and other well-known services (such as SMTP, FTP, SIP, etc.) against attacks embedded in the application content and flows, and to minimize the probability of using such services as entry points to launch attacks. The used techniques or implemented network designs should ensure the ability of inspecting encrypted traffic.
5. DNS service should be split; the service resolving incoming queries from the outside is separated from the service resolving inside queries.
6. Running DHCP services should be authorized. Network should be monitored to detect any unauthorized service running in the network.
7. The network should be configured in a manner that ensures registering and approving all wireless access points and base stations that are connected to the enterprise network. Settings and configuration should ensure allowing only permitted terminals to connect securely. Network should be monitored to detect and then deactivate any unauthorized or rogue devices.
8. The entity should implement the protection measures against L3/L2 network attack techniques such as ARP poisoning, MAC spoofing, DHCP Spoofing, etc.

9. Periodically (at least twice a year) and on a change basis, a review process for applied rules and configurations should be conducted and documented.

G.6.2. System and Application Hardening

The entity has to maintain, implement and communicate system and application hardening procedures to ensure secure configuration.

1. All systems and applications must be hardened in accordance with vendors and industry-standard security guidelines. Hardened configuration can be overruled by application-specific configuration requirements to maintain a proper operational state.
2. The administrators should consider performing at least the following steps:
   2.1 Servers should be on a dedicated, single-purpose host.

   Example: don't run both web and DNS services on the same computing machine (i.e. physical server, VM or container).

   2.2 Remove all unnecessary components, or disable those that cannot be removed. Also, install the minimal OS configuration and then add, remove, or disable components as needed. Such components are:
   - System features and subsystem modules
   - Applications, application modules, application packages, and add-ons
   - Services
   - Drivers and firmware
   - Scripts
   - Network protocols (e.g. IPv4, IPv6, SMB, NFS, Telnet, etc.)

   Example: disable OS features and services such as "File and Printing Services on Microsoft Windows" if they are not required for the running application.

   Example: install Microsoft "Server Core" if there is no need for "Desktop Experience".

   2.3 For privileged computing machine, the network should ensure no access to the services that are potentially considered as entry points and exit points for threats, and also might be used for data leakage or establishing covert channels such as Internet and email services. Also, initiating network connections from trusted zones and servers should be restricted on as-needed basis.

   2.4 Systems should be configured and tuned to run application instances, processes and services under restricted credentials and accounts, where access to system resources is granted on as-needed basis.

   2.5 Whitelisting only predefined trusted applications to run on the system.

   2.6 Disable all interactive logon capabilities for non-interactive logon accounts.

   2.7 Rename default administrative accounts to the possible extent, change all system and application default passwords, and remove or disable unnecessary user accounts.

2.8 Set auto-lock options for computing machines. At most 15-minute inactivity time-out is recommended.

2.9 Change all default SNMP community strings and encryption keys.

2.10 Restrict physical ports (such as USB).

3. Deviations from the selected hardening configuration standards and applied mitigation controls are documented and justified as a part of the configuration management process.
4. Periodically – at least twice a year – and on a change basis, a review process for configuration settings must be conducted and documented.

G.7. Remote Access

G.7.1. Remote User Access

The entity has to maintain, implement and communicate remote user access policy and procedure. The policy and procedures should at least address:

1. Granting remote access permissions and time windows must be based on business needs.
2. Remote access to information assets and resources must pass through end-to-end secured tunnels (i.e. TLS or IPSec) that are established over the public network (i.e. Internet). Established tunnels must be terminated on a well-controlled and specific-purpose network zone located at the boundaries before passing the incoming traffic to the internal network.
3. Remote access tunnels must be secured using strong cryptographic mechanisms and standards.
4. Working only on company-issued machines to the possible extent, and apply authentication mechanisms to authenticate the machine (e.g. based on digital certificate).
5. The entity has to consider the principles of Zero Trust Architecture (ZTA) for the company-issued machines when being moved outside the enterprise network for remote access, as well as for BYOD when being used for remote access.
6. Applying at least two-factor authentication mechanisms to authenticate the users before accessing internal information assets and resources (i.e. at the tunnel endpoint). Authentication services for identities used to authenticate remote users at tunnel endpoints should be separated from the identities used to access other information assets and resources internally.
7. Copying, moving, and storage of classified data and information onto local hard drives and removable electronic media must be prohibited, unless explicitly authorized for a defined business need.
8. Updating and patching remote machines must be ensured. Unpatched machines should be quarantined and remediated before accessing internal information assets and resources.
9. Deployed technology should ensure disconnecting inactive sessions, and destroying all agreed upon encryption keys after terminating or disconnecting the session.
10. Restrict uncontrolled user access to Internet during the remote access session.
11. Personal firewall or equivalent functionality should be installed, configured properly and always kept running on the remote machines.
12. Educate end users to avoid connecting remote machines to public wireless networks and not leaving the machines unattended in public areas.
13. Set boundaries for meetings that are conducted online to keep the privacy of discussions.
14. Remote access of external support staff must be granted on a temporary basis and time limited to actual business needs. Also, remote access sessions to be recorded and monitored to the possible extent.

Granted remote control during the session should not to be left unattended. Also, trusted remote access and control tools should be predefined and preauthorized.

15. Periodically – at least twice a year – and on a change basis, a review process for configuration settings must be conducted and documented.
16. Remote access activities must be logged and monitored.

G.7.2. Site-to-Site Access

The entity has to maintain, implement and communicate procedures for enabling site-to-site access between branches, with trusted partners and with services hosted on cloud. The procedures should include:

1. Configuring site-to-site access and topology in a manner that ensures permissions and time windows are granted based on business needs.
2. Site-to-site tunnels must be secured using strong cryptographic mechanisms and standards.
3. The authentication between peers and endpoints should be based on digital certificates instead of pre-shared key mechanism.
4. Periodically – at least twice a year – and on a change basis, a review process for configuration settings must be conducted and documented.
5. Site-to-site access activities must be logged and monitored.

G.8. Cryptography

G.8.1. Key Management

The entity has to maintain, implement and communicate key management procedures to ensure managing cryptographic keys securely during the entire lifecycle.

1. The procedures should be guided by international standards and best practices. Recommended sources are the latest published revisions of related **NIST** special publications.
2. Generally, the procedures should consider:
   - 2.1 Avoid generating and storing cryptographic keys using weak algorithms, or in insecure locations or stores. In addition, keys must be stored in the fewest possible stores. Also, crypto operations on the keys must be performed within the secure stores.
   - 2.2 Key-encrypting keys must be stored separately from data-encrypting keys. Also, data-encrypting keys should not be stored in the same store of the encrypted data sets.
   - 2.3 Cryptoperiod of keys must be specified. Process to rotate expired keys must be established and maintained.
   - 2.4 Distributing keys only to required or preauthorized users and services. Keys must be distributed through secure channels separate from data channels.
   - 2.5 Assigning key components to authorized custodians should be maintained in a unified inventory.
   - 2.6 Avoid using the same keys across development, testing and production environments.
   - 2.7 A backup/recovery process for the keys should be defined. The process should ensure protecting backed up keys against unauthorized access, loss of integrity and damage. In addition, key recovery should be recorded.
   - 2.8 Compromised keys must be rotated and revoked. Rotated and revoked keys must be securely archived, then destroyed and purged permanently from all key stores. Archived keys must be only used for decryption operations.
   - 2.9 Avoid hard-coded keys.
   - 2.10 Key lifecycle portions should be automated to the possible extent.
   - 2.11 Splitting the keys when storing and distributing into multiple portions where applicable.
   - 2.12 Ensuring segregation of duties in key management operations to the possible extent.

G.8.2. Mechanisms

The entity has to maintain, implement and communicate a practice for using cryptographic standards and mechanisms to ensure the use of strong cryptographic keys, algorithms and protocols. The practice could be developed based on adopting international standards and best practices. Recommended sources are the latest published revisions of related **NIST** special publications.

Generally, practice should consider the following algorithms and key lengths:

1. Symmetric block-cipher cryptographic algorithms and key lengths (encryption/decryption and key wrapping/unwrapping):
   - AES-128, AES-192 and AES-256.
2. Asymmetric digital signature generation and verification algorithms and key lengths:
   - DSA: (L, N) = (2048, 224), (2048, 256) or (3072, 256) bit
   - ECDSA: len (n) ≥ 224 bit
   - RSA: len (n) ≥ 2048 bit
3. Random bit generation algorithms (e.g. generation of keys, nonces and authentication challenges):
   - Hash_DRBG and HMAC_DRBG
   - CTR_DRBG with AES-128, AES-192 and AES-256
4. Hash functions for all applications:
   - SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)
   - SHA-3 family (SHA3-224, SHA3- 256, SHA3-384, and SHA3-512)
5. Message Authentication Code algorithms:
   - HMAC generation and verification: key lengths ≥ 112 bit
   - KMAC generation and verification: key lengths ≥ 112 bit
   - CMAC generation and verification: AES
   - GMAC generation and verification: AES
6. Key exchange and agreement algorithms:
   - DH Group 14, len (n) ≥ 2048 bit
   - ECDH Group 19, lengths ≥ 256 bit
   - RSA: len (n) ≥ 2048 bit

G.9. Logical Monitoring and Detection

G.9.1. Network Monitoring

The entity has to implement detective mechanisms for monitoring network topology, flows and usage and detect deviations from baselines. The entity should:

1. Detect unusual utilization and consumption of network resources and bandwidth (e.g. upload Internet bandwidth). The monitoring process should be granular (e.g. per user/source and network session).
2. Collect network flow information. A baseline of network flows should be built and maintained, deviations of the flows should trigger alerts.
3. Capture network packets in a manner that enables rebuilding network sessions. Scoped segments and retention period for the captured packets should be determined based on a risk assessment process.
4. Detect rogue access points and rogue network traffic. Also, changes of topology of L2 and L3 networks and site connections should be detected.

G.9.2. Personnel, Device and Service Activities Monitoring

The entity has to implement detective mechanisms for monitoring personnel, device and service activities in order to detect deviations from baselines. The entity should:

1. Monitor user and service activity at the levels of network, operating system, service and application. Monitoring and logging should at least include:
   1.1 Logon operations such as:
   - Failed logon attempts and account lockout frequencies.
   - Interactive logon attempts of service accounts.
   - Logon attempts with privileged accounts and vendor default accounts.
   - Logon attempts with disabled or expired accounts.
   - Logon attempts with decoy accounts.
   - Frequencies of logon attempts by day, by time (e.g. outside business hours), by location (e.g. logon from a location never being used before), and by device (e.g. same account from multiple sources or multiple accounts from the same source).
   - Types of logon attempts (e.g. interactive, as a service, etc.)
   - Time since last logon.

   1.2 Elapsed time per session.
   1.3 Execution and CRUD operations frequencies and denials.
2. Monitor authentication services and user alteration operations. Monitoring and logging should include:
   - Creating, updating and deleting credentials. Creating and then deleting credentials within short periods and creating/deleting bulk of users within short periods should be alerted.
   - Password changes. Multiple password changes within short period should be alerted.
   - Privileged group membership changes.
3. Monitor failed access attempts. Monitoring and logging should be at the levels of:
   - Network, such as hitting explicit or implicit deny access rule, failed logon into network admission control, failed logon into remote access endpoint, etc.
   - Operating system, firmware, application and information resource.
4. Monitor operational status changes of the systems, services and applications (e.g. restart, stop, file system full, etc.).

G.9.3. Detecting Malicious Activity

The entity has to implement detective mechanisms for monitoring malicious activities. The entity should:

1. Implement signature-based and behavioral-based intrusion prevention solutions at both, network and host levels.
2. Implement network-based and host-based, signature-based and behavioral-based antivirus and malware analysis solutions.
3. The entity should provide DoS and DDoS (volumetric and non-volumetric) mitigation services to protect critical published services over Internet.
4. The used detective techniques and implemented network designs should ensure the ability of inspecting encrypted traffic.
5. Enable the monitoring and logging of:
   - 5.1 Events of warning, rejection and blocking actions on inline and promiscuous, host and network-based intrusion detection and prevention systems.
   - 5.2 Events of warning, rejection and blocking actions on host and network-based antivirus and malware-analysis technologies.
   - 5.3 Events of warning, rejection and blocking actions taken by data leak detection and prevention tools.
   - 5.4 Presence of hacking tools.
   - 5.5 Unusual utilization and consumption of system resources, as well as system crashes. Granularity levels in monitoring and collecting statistics to be per user session and per process are highly recommended.
   - 5.6 Access and modification to system and application logs, configuration, setting and repositories (e.g. Windows registry).
   - 5.7 Logs and alerts generated by integrity check tools.
   - 5.8 Service-level access activity such as:
     - Strings of requests and responses to a web service resource.
     - DNS outgoing and incoming queries
     - DHCP requests and leases
     - Reported phishing emails and email service usage
   - 5.9 Access to logs and events, clearing logs, as well as modifying logging settings.

G.9.4. Detecting Unauthorized Code Installation and Injection

The entity has to implement procedures to control the installation of software on operational systems whether systematically or manually. The procedures should at least ensure:

1. Formal change management procedures have taken place. The below steps should be ensured before the installation on operational systems:
   - Trust of software issuer should be verified through validating document code signing certificates and the digital signatures of the executables where applicable.
   - Integrity check processes have to ensure detecting and logging or alerting changes or unexpected additions to software executables and libraries.
   - Checking software against malware infection or enabling malicious activity. Malware analysis techniques (such as sandboxing) can be deployed to achieve it.
   - Not introducing capacity, performance and business operation issues.
2. Restricting the ability of users to install software, especially on local devices. Whitelisting approach could be implemented to specify what software and programs can be installed and run.

G.9.5. Vulnerability Scanning and Penetration Testing

The entity has to establish and maintain vulnerability scanning and penetration testing processes. Generally, following should be taken into consideration:

Vulnerability scanning process:

1. Define the frequency of performing vulnerability scanning processes. Scanning frequencies should be specified according to the criticality and sensitivity of the systems, in addition to best practices, related regulations and industry rules. It is highly recommended to be conducted at least once a month for critical and sensitive systems.
2. Define the scope of each scanning process, which should include at least:
   2.1 Systems and infrastructure components within the scope.
   2.2 The breadth and depth scanning coverage for each system. Breadth is the percentage of components or number of vulnerabilities to be checked, while depth is the level of the system design to be checked.
3. Vulnerability scanning process should include scanning for ports, protocols, functions, services, underlying operating system and components, and patch levels. Scanning should be performed bypassing and through the applied controls to ensure that they are properly configured and operating correctly.
4. The scanning tool should:
   4.1 Express vulnerabilities in CVE naming convention and express vulnerability impact by CVSS.
   4.2 Employ OVAL to determine the presence of vulnerabilities.
   4.3 Use sources include CWE and NVD lists for vulnerability information.
   4.4 Be SCAP validated.
5. Vulnerability scanning process should include extensive search and discovery for classified data and information that adversaries could obtain without compromising or breaching the system.
6. Vulnerability scanning process should consider privileged access authorization to assets within the scope to facilitate vulnerability scanning thoroughly.
7. As part of the vulnerability management, the entity should:
   7.1 Use automated mechanisms to analyze multiple vulnerability scans over time to determine trends in system vulnerabilities and identify patterns of attacks.
   7.2 Review historic audit logs to determine if recently detected vulnerabilities in the systems have been previously exploited by attackers.
   7.3 Correlate the output from vulnerability scanning processes to validate the presence of multi-hop attack vectors that have been identified by threat modeling process.

Penetration testing process:

8. Define frequency of performing penetration testing processes. Test frequencies should be specified according to the criticality and sensitivity of the systems, in addition to best practices, related regulations and industry rules.
9. Define the scope of each testing process.
10. Use the results of vulnerability scanning process to support penetration testing
11. Independent penetration testing team has to be managed by Information Security Management to perform the process. Rules of engagement and contracts should be communicated, and classified data and information should be protected.
12. Testing should be performed bypassing and through the applied controls to determine the degree of penetration resistance to attacks. Also, it should consider performing attempts to bypass implemented physical security controls.
13. The testing process should consider performing technology-based attacks (e.g. interactions with systems and business processes), and social engineering-based attacks (e.g. interactions via email and telephone). Also, it is highly recommended to conduct tests taking into account adversarial tactics, techniques, procedures, and tools.
14. Protecting data and service continuity during performing aggressive vulnerability scanning and penetration testing processes must be considered to ensure no service interruption and no data loss.

G.10. Event Data and Evidences

G.10.1. Clock Synchronization

The entity has to deploy time synchronization mechanism for all IT and security systems. The following have to be ensured:

1. Existence of central time service(s) for the enterprise where all systems are configured to sync the time information with.
2. The time of central time service(s) should be synced with at least two trusted national/international sources.
3. Designated time sources are based on UTC.
4. Confidentiality and authenticity of exchanged time information should be protected.
5. Time setting logs on servers must be reviewed and monitored.

G.10.2. Events Sources, Collection and Tracing

1. Define event and log source points on-premises and on cloud. Source points should include at least:
   1.1 Cybersecurity technical controls such as firewalls, intrusion detection and prevention systems, application control, antivirus, malware analysis tools, data leak detection and prevention systems, network admission control, remote access endpoints, and integrity check tools.
   1.2 Server and client operating systems
   1.3 Applications, RDBMSs and file repositories
   1.4 Application underlying services (e.g. web server)
   1.5 Authentication services
   1.6 Network devices such as switches, routers and access points.
   1.7 Network services (e.g. DHCP, DNS, Email service, etc.)
   1.8 Physical control systems
2. Define what to collect from each source. Collected events and logs information should contain:
   - Who: user ID
   - When: date and time. All collected logs and events must be timestamped with dates and times synced with the central time service
   - From/to where: source and destination of activity (location, IP address, hostname, process ID, service name, etc.)
   - What: Details of event and the action whether successful or failed.
3. Log retention:
   - Events and logs should be accessible and searchable for at least one year.
   - Captured data network packets should be available to rebuild sessions for at least two weeks.
4. Vulnerability status, and missing patches and updates of systems and applications.
5. Periodically (at least twice a year), and on a change basis, a review process for logging settings should be conducted and documented.

G.10.3. Analysis and Correlation

The entity has to ensure that:

1. Logs and events are collected into a secure unified repository separated from log sources. A process must be implemented to ensure the integrity of the log repository, and to ensure not permitting IT admins to manipulate collected logs.
2. Collected log and event information from different sources should be parsed into a uniform format to facilitate building analytic and correlation rules. Collected raw logs should not be deleted and must be kept.
3. A playbook should be maintained to define the use cases to be translated into continuous and on-demand analytic and correlation rules to enable early detection of malicious activities.
4. The ability of adding context and enrichment data to achieve actionable intelligence.

G.10.4. Alerting and Event Management

The entity has to maintain a documented event management process that address classification criteria of observed activities (event or series of events) as an incident, as well as the reporting and escalation path of the observed activities. Classification criteria should consider at least:

1. The observed activity or activities indicative of a security breach with high chance of success.
2. The progression stage of the threat action in the observed activity or the event. Stage categories could be:
    - Preparation in which the actor uses reconnaissance techniques such as port scanning and sending phishing emails.
    - Engagement in which the actor starts delivering malicious payloads, exploiting vulnerabilities and interacting with the systems and applications. The event should be considered as an incident from the moment of starting delivering malicious payloads.
    - Presence in which the actor starts establishing and maintaining:
        - Control and backdoor channels (Command and Control).
        - Unauthorized data connections, transfers, or modification, as well as unauthorized communications within the network (Lateral Movement).
        - Persistence by placing unauthorized services and processes in the operational environments.
    - Effect in which the actor starts lateral movement and perform attack objectives.
3. The location (e.g. internal network, DMZ, etc.), the affected elements in the observed activity, and the asset values and the classifications of the affected elements.
4. Actor characterization where applicable

G.11. Cyber Threat Management

The entity has to establish and maintain threat intelligence processes to ensure the understanding of emerging and targeted cyber threats. The process should include:

1. Identifying and collecting potential threat information from:
   1.1 Internal sources such as logs of detective and preventive cybersecurity and fraud controls, as well as deliverables of threat modeling, risk management, audit and compliance processes.
   1.2 External sources such as:
   - FinCERT and other national CERTs and government agencies
   - International CERTs
   - Open sources such as **OSINT**.

     MITRE ATT&CK Enterprise and Mobile Tactics and Techniques can be used to define and understand different threat actors (APT groups), motivations, tactics and techniques.
   - Reliable commercial sources and service providers
2. The methodology, the tools and periodicity of correlating and analyzing threat information, as well as derive actionable indicators of compromises for each identified threat. Derived and collected IoCs should be applied and injected into running detective and preventive cybersecurity and fraud controls.
3. Sharing relevant intelligence information with FinCERT.

G.12. Mobile Devices

G.12.1. BYOD

The entity has to ensure the protection of classified data and information during transmission and storage when using personal devices.

1. Enabling access to the entity's enterprise network resources from devices that are not owned or configurable by the entity (i.e. BYOD) must be designed with zero trust tenets.
2. Define user responsibilities, and conduct awareness sessions about BYOD security risks, applied cyber security controls on personal devices, and the restrictions and consequences for employees.
3. Enroll and manage BYOD with mobile device management (MDM) solution that enable:
    - Applying security controls seamlessly.
    - Applying isolation techniques (e.g. containerization) to separate corporate information and application from personal information.
    - Applying access controls and encryption mechanism to corporate container, as well as preventing unauthorized data leaks.
    - Remote wiping for managed data, information and applications.
4. Limit the number of BYOD devices used by each employee based on business needs.
5. Preapprove public and third-party mobile applications that can access to corporate information assets.
6. Block access from lost, rooted or jailbroken devices, as well as terminated employees.
7. BYOD access activities must be logged and monitored.

G.12.2. Portable Devices

In addition to applicable controls mentioned in section [G.12.1], the entity has to ensure mitigating the risks of using portable devices.

1. Permitting portable devices to access enterprise network after authorization. Security health check for portable devices should be performed prior to granting access to the enterprise network. Unhealthy devices should be quarantined and remediated before accessing internal resources.
2. Security controls must be applied and ensured before provisioning the portable devices.
3. The portable device should be tagged to a unique individual, and number of devices tagged to each individual should be limited based on business needs. Portable devices of terminated or end of service individuals must be returned. Data residing on returned devices must be securely erased or backed up as needed.
4. Only preapproved software and applications are installed and running on the portable devices.
5. Controls such as disk encryption and remote wipe should be applied.
6. Portable devices access activities must be logged and monitored.

G.13. Maintenance

The entity should ensure that:

1. All critical IT and security assets are under valid maintenance or service delivery agreements that involve response and recovery terms and conditions aligned with the levels of the business criticalities.
2. Conducting preventive maintenance and health checks periodically to ensure performance as per intended purpose and specifications.

H. Electronic Services

When delivering electronic services, the entity has to consider related CBJ, national and international regulations and standards to ensure data security. Controls under this section should be considered as minimum.

H.1. Financial Transactions

The entity has to ensure the security of financial transactions and messages whether at-rest, in-use, or in-transit by considering at least the measures mentioned in section [G.4] and other parts of the framework, as well as related national and international regulations and standards mentioned in section [C]. In addition, the entity has to ensure:

1. All financial transactions and messages must be identified using unique reference numbers to enable traceability.
2. Monitoring of customer transactions throughout the day, and should consider the following factors:
   2.1. Preconfigured limits in terms of amounts and frequencies.
   2.2. Frequency of the transactions, and time intervals in between in a way that can detect spikes in volumes and whether the individual transactions are performed by human, by a robot or code.
   2.3. Failed authorization attempts prior to initiating the transaction.
   2.4. Predefined fraud scenarios.

   Fraud detection and prevention measures should provide an enterprise view across all retail payment activities that use multiple payment channels for processing and clearing.
   2.5. Abnormal payment patterns in relation to the costumer's profile and history.

   Establishing a baseline of the customer behavior should consider at least transaction participants, amounts, frequency, and timing.
   2.6. Changes related to sensitive information of the customers.
   2.7. Location of the payer and the beneficiary.
3. Implement business controls to detect and prevent suspicious payment and transfer activities such as:
   3.1. Conducting effective **daily** reconciliation process to verify and validate the integrity of information processed through electronic payment channels and to identify differences.

   For SWIFT transfers, the entity should review the received statement messages in order to check that the amounts and balances recorded on the statements match their own records of transaction activity.
   3.2. Real time monitoring for payment activities, and taking appropriate precautions before credit limits or debit caps are exceeded, or when their business practices may indicate possible fraud.

3.3. Managing what payment and transfer message types are permitted to be exchanged with counterparties and correspondent banks.

3.4. Providing transfer confirmation, and requiring counterparty and correspondent bank to send confirmation messages.

3.5. Having policies in place around payment amendments and rapid cancelation. Cancelation should be for the original instructions or via sending payment adjustments for not impeding reconciliation.

H.2. Service Delivery

H.2.1. Online Banking

1. The entity has to ensure secure delivery of customer credentials and perform authentication of customer devices. Also, the entity should implement additional authorization factors for account activation, password reset, financial transactions, new beneficiary addition, and beneficiary modification using:
   - Out-of-band one use secrets, where the secret is sent by the entity through a channel and verified by the individual through another channel (e.g. OTP over SMS to the registered customer phone number).
   - Offline or online, time-based or hash-based OTP (hardware or software).
   - Cryptographic authenticator (hardware or software) (e.g. cryptographic smart card or token).
   - Validity of one-time secretes must be restricted to a maximum of five minutes.
2. For mobile and web banking services, the entity should ensure:
   - Adopting resiliency by design security principles when developing mobile and web banking applications.
   - The mobile application verifies the mobile number and device IMEI or ESN of the customer and customer's device for first time use of applications
   - User session is terminated after maximum 5 minutes of inactivity.
   - Concurrent sessions are prohibited, but may access from up to three validated devices.
   - Techniques to protect against MiTM attacks, such as TLS pinning.
   - Use EV TLS digital certificates, in addition to deploying additional controls to assist the customer in identifying phishing sites.
   - Avoid caching sensitive data on customer's device, encrypts the data stored – if any – by the application on the customer devices.
   - Prevent installing the mobile banking application on rooted or jailbroken devices.
3. The process for changing the customer mobile phone number should be done from ATM or through direct interaction with the customer either in a branch or remotely over a secure and trusted channel.
4. Use of brand protection measures to protect online services including social media.
5. Scheduled downtime of the Internet banking services should be timely communicated to the customers. The entity should analyze and assess the impact of the scheduled downtime, and determine the threshold, after which, the entity should notify the customers.

H.2.2. Self-service machines and PoS/PoI

The entity has to consider self-service machines (e.g. ATM) and PoS/PoI as unattended assets, and has to ensure their security, in addition to the security of all exchanged data, by considering at least the measures mentioned in this framework, and related national and international regulations and standards mentioned in section [C]. Additionally, the entity has to ensure at least:

1. Implementing anti-skimming and PIN-pad protection solutions.
2. Authenticating customer transactions – depending on the transaction characteristics and acceptable risk levels – using combination of at least two-factor authentication such as:
    - Card, either physical or tokenized, and memorized secret (e.g. PIN), either static or one-time.
    - Physical biometric methods and memorized secret.
3. Detecting exploiting attempts of the machines applications and infrastructure vulnerabilities.
4. Implementing video monitoring and physical security measures to protect the machines from theft, damage, etc.
5. Remote stopping of machines in case of malicious activity detected.
6. Performing periodic physical inspection of the machine locations to verify the effectiveness of implemented security measures.

H.2.3. Contactless Payments

The entity has to implement controls to protect the security of contactless traffic exchanged between customer device and the transaction touchpoint.

1. The entity has to conduct a risk assessment process to identify any raised security risks due to the use of NFC and QR code technologies, and then implement the most appropriate controls to mitigate identified risks. Risk assessment process should at least address the following risk factors:
    - Eavesdropping
    - Data insertion, manipulation and corruption attacks
    - MiTM and relay attacks
    - Skimming and spoofing attacks
    - Reading malicious content
    - Stolen customer devices
2. Number and value of NFC transactions should be limited. Any subsequent transactions should enforce additional authentication.

H.2.4. Other Service Delivery Channels

The entity may deliver services over mailing channels (e.g. email, fax, human courier, etc.), over texting channels (e.g. SMS/USSD, and open mobile application such as WhatsApp), through service-to-service APIs, and over phone calls. The entity has to ensure exchanged data security by considering at least related measures mentioned in section [G.4] and other parts in the framework. Additionally, the entity has to ensure:

1. Verifying and validating high risk financial and non-financial transactions through a second out-of-band trusted channel as applicable.
2. Implementing measures to ensure that personal identity verification over phone calls are neither generic nor easy to obtain (such as from notification messages) or repeated.
3. Implementing techniques that detect and prevent impersonating and spoofing scenarios, and ensuring that a transaction is generated from the genuine source in a way that also protect against man-in-the-middle attacks.
4. Implementing techniques that assist customers to identify phishing services.
5. Minimizing sensitive information exchange over the channels.

H.3. Payment Cards Operations

1. Segregation of duties must be implemented for payment card personalization and processing, PIN generation and delivery of the card and PIN to the customer.
2. Payment card PIN generation must be secured, and access to PIN is restricted only to the intended recipient.
3. Payment cards must be issued in inactive state and activated through an approved process after being received by the customer.
4. Customers have to be provided with appropriate channels or facilities to block their payment cards by themselves or through customer service center.
5. Access to electronic payment service and payment cards must be blocked and revoked after maximum of three failed authentication or authorization attempts. Procedures must be defined to reactivate blocked accesses considering an enhanced process of due diligence and customer identity verification through secure channels.

H.4. Customer Notification

The entity should ensure that:

1. All notifications are sent to pre-registered and pre-verified effective channels, contact numbers and addresses of the customers.
2. Changes to customer identification and contact information such as mobile phone number and email address must be performed only after the authenticity of the customer is ensured, and the customer is authenticated using multi-factor authentication when changing request is performed through an electronic channel. Alerts and the second factor authentication should be sent to old contact phone number or email address until authorizing the change.
3. Customers have to be notified about:
   2.1. All transactions performed on their accounts, including rejected and reported unusual transactions.
   2.2. Changes to pre-set defaults and values such as password, limits, etc.
   2.3. Card status changes.
   2.4. Adding new beneficiary or modifying and existing one.
4. The entity has to ensure sensitive data is not disclosed in notification messages such as account and card numbers.
5. The entity should launch awareness programs and campaigns by suitable channels to customers, and cover the minimum aspects below:
   5.1. Not to share passwords, secrets, and PINs with anyone over any channel even the bank itself.
   5.2. Choose complex passwords.
   5.3. Notifying the bank immediately after changing any of contact or identification numbers or addresses.
   5.4. Avoid installing any mobile banking application except from trusted stores (i.e. Google and Apple stores).
   5.5. Avoid installing untrusted suspicious and gaming applications on the same device where mobile banking application is installed.
   5.6. Not to leave the mobile phone or hardware authenticators unattended.
   5.7. Not to expose or reveal any sensitive information about their accounts when interacting with bank ads and posts on social media networks.
   5.8. Not to click any link or open any attachment in received text messages or emails that impersonate the bank identity before verification.

H.5. Digital Onboarding

When delivering digital onboarding service, the entity should consider the following measures:

1. Provide mechanisms to protect against falsified identity spoofing and forged evidences through at least:
   - Validating physical security features of presented evidences.
   - Extracted data from barcodes and machine readable zones of presented evidences are compared to the extracted OCR data.
   - Validating gathered personal details in the evidence with the issuer of the evidence or authoritative source.
2. Provide mechanisms to protect against fraudulent use of identities of others. Mechanisms can include:
   - Match the live selfie captured against the photo on the identity evidence automatically.
   - Verifying identity evidence, captured face images and biometric of applicant against information obtained from authoritative source.
   - Verifying applicant provided nongovernment-issued documentation (such as electricity bills) to help achieve a higher level of confidence in the applicant's identity
3. Deployed digital onboarding technology should ensure a person can enroll only once depending on biometric deduplication check during enrollment.
4. Deployed face recognition algorithm should ensure near-perfect accuracy. The entity can rely on a tested algorithm based on **NIST Face Recognition Vendor Test (FRVT)** program.
5. Deployed digital onboarding technology has to ensure providing liveness detection mechanism. Liveness detection mechanism should be tested to meet the standards of **ISO/IEC 30107-3 for Presentation Attack Detection**.
6. In case of deploying predictive algorithms (i.e. AI and ML) for identification, verification, and automating decision-making process; the entity should ensure minimizing False Acceptance Rates (FAR) or False Positive Rates (FPR) to values tolerated based on the entity's risk assessment outcomes. It's recommended that overall FAR/FPR does not exceed 5% over any sampled period of time.

Confusion Matrix		**Identification and Verification Result**	
		Accepted	**Rejected**
Applicant	**Genuine**	True Positive	False Negative
	Imposter	False Positive	True Negative

$$\text{FAR} = \text{FPR} = \frac{\text{no. of False Positives}}{\text{no. of False Positivies} + \text{no. of Truse Negatives}} x\ 100\%$$

7. Digital onboarding technology should provide location capturing. Captured locations should be considered for address verification and fraud detection means.
8. Enrollment repudiation through at least saving a subscriber's biometric, video conference and/or a trusted digital signature linked to a certificate issued by an authorized entity.

I. Third Parties

I.1. Contractors and Vendors

The entity should define a process to identify, assess, manage and mitigate the security risks of supply chains, contractors, vendors, outsourcing and third-party service providers.

1. The contractual agreements with third parties must state the responsibilities for cybersecurity for all parties. The contractual obligations for third parties must reflect the entity's policies for cybersecurity, in addition to clarifying and stating:
   - Third party who is granted access to non-public information should sign a confidentiality or non-disclosure agreement (NDA) prior to being granted the access. This NDA should be identified, regularly reviewed and documented.
   - Description of the information to be provided or accessed and methods of providing or accessing the information.
   - Third party's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation.
   - Responsibilities for classifying information and managing assets.
   - Actions to be taken if the third party disregards the entity's security requirements.
   - Screening requirements for third party's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed, or if the results give cause for doubt or concern.
   - Obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing.
   - The requirements to address the information security risks associated with information, business information transfer, and communications technology services as well as supply chain.
   - Incident management requirements and procedures (especially notification and collaboration during incident remediation) in issues related to the third party.
   - Service levels and management requirements of all third party provided services.
2. For IT service outsourcing, outsourcing policy should be developed, maintained and implemented. The policy should at least address:
   2.1. Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the entity.
   2.2. IT service outsourcing agreements must be inventoried. Agreements should define and include:
      - Clear scope of services and service level requirements

- Minimum requirements of operations, cybersecurity, risk management, and business continuity, as well as notifications and disclosures of data breach events.
- Roles and responsibilities for implementing cybersecurity requirements.
- Right to audit and inspect.
- Termination clause and exit plans that consider secure retrieval and/or disposal of information assets exchanged during the execution of the agreement.

2.3. Security requirements of the agreement shall be reviewed and updated periodically or upon significant changes in services provided by third party vendors.

2.4. Cyber risk management processes of service providers are identified, established, assessed, managed, and agreed to by relevant stakeholders.

2.5. Proper due diligence and assessment for service providers during the selection process and regularly thereafter using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. Selection process should cover:

- Experiences and capabilities of the third-party staff.
- Financial position.
- Available internal control environment, cybersecurity standards and practices, and BCP and DR arrangements.
- Compliance with applicable laws and regulations.

2.6. Risk assessment shall be conducted for outsourced services as per the risk management process.

3. Entity should require third parties to notify the entity of any personnel transfers or terminations who possess entity credentials and/or badges, or who have system privileges.
4. Entity should monitor, review and audit third party service delivery and compliance with entity security requirements and the contractual obligations, and activity to detect potential cybersecurity events.

I.2. Cloud Security

In addition to section [I.1], the entity has to ensure that cyber risks are assessed and addressed, and the principles and controls of Zero Trust Architecture (ZTA), CSA, ISO 27017, and ISO 27018 are deployed for cloud services where applicable. Cloud security measures must be developed, documented and maintained. Those measures should be guided by CBJ published guidelines and international practices**.** Developed measures should consider at least the following:

1. Extending organizational policies, procedures, standards and practices that are related to application development, service provisioning, service design, service implementation, service testing, service use, and service monitoring to include the cloud environment. Audit mechanisms and tools should be defined to ensure that organizational practices are followed.
2. Establishing a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of systems and applications.
3. Assessing the impact of cloud computing initiatives on the compliance with laws and regulations that impose privacy and security obligations on the entity. Particularly, those initiatives involving data location, privacy and security controls, records management, and electronic discovery requirements.
4. Ensuring that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
5. Clearly stating the exclusive ownership rights of the entity over data.
6. Ensuring the sufficiency and suitability of data protection measures through:
    - Evaluating cloud provider's data management solutions and the ability to control access to data, to protect privacy, to secure data while at rest, in transit, and in use, and to sanitize data.
    - Taking into consideration the risk of collating entity data with that of other entities whose threat profiles are high or whose data collectively represent significant concentrated value.
    - Fully understanding and weighting of the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
    - Ensuring the existence of controls to protect against data loss or leakage. These controls should include at least implementing strong API access control and analyzing data protection at both design and run time.
7. Ensuring that cloud provider offerings and contract terms of data CIA, incident response, disaster recovery and business continuity procedures meet the contingency planning requirements of the entity. Also, contract terms should ensure right to audit and inspect including rights to audit for CBJ.
8. Engaging with cloud providers that have protection against abuse and nefarious use of cloud computing, and at least deploy:

- Stricter initial registration and validation processes, and offer limited and well controlled free trial services especially for PaaS services.
- Enhanced card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for network blocks.

9. Ensuring protection against malicious insiders. The entity should ensure that:
   - The cloud provider enforces a strict supply chain management and conduct a comprehensive supplier assessment.
   - Human resource requirements are enforced as part of legal contract, in addition to requiring transparency into overall information security and management practices, as well as compliance reporting.
10. Ensuring that cloud provider provides secure interfaces and APIs through:
    - Analyzing the security model and safeguard controls in place of cloud provider interfaces.
    - Ensuring that strong authentication and access controls are implemented in concert with encrypted transmission.

      In identity federation scenarios with the cloud provider, identity and access management transactions must be interpreted carefully and unambiguously and protected against attacks. In addition, clear separation of the managed identities of the entity from those of the cloud provider should be ensured to protect the entity's resources from provider-authenticated entities and vice versa.
    - Understanding the dependency chain associated with the APIs.
11. Ensuring that cloud provider has controls in place to mitigate shared technology issues by at least:
    - Deploying logical isolation and virtualization techniques. Employed isolation techniques in multi-tenant software should be clearly understood and the risks involved for the entity should be assessed.
    - Implementing security best practices for installation and configuration
    - Monitoring the environment for unauthorized changes and activities
    - Promoting strong authentication and access control for administrative access and operations
    - Enforcing SLAs for patching and vulnerability remediation
    - Conducting vulnerability scanning and configuration audits.
12. Ensuring the protection against account or service hijacking and stealing credentials by at least:
    - Prohibiting the sharing of account credentials between users and services.
    - Leveraging strong two-factor authentication techniques where possible.

- Employing proactive monitoring to detect unauthorized activity.
- Understanding cloud provider security policies and SLAs.

13. Unknown risk profile due to the lack of knowledge of cloud provider's protocols and policies should be addressed by at least:
    - Defining the roles and responsibilities involved in managing risks.
    - Ensuring that service arrangements have sufficient means to allow:
        - Full or partial understanding of applicable underlying infrastructure details that are being used to provision services.
        - Visibility into security and privacy controls, employed processes, as well as the performance over the time.
        - Obtaining logs, monitoring and alerting on necessary information.
14. Ensuring that the cloud provider has a transparent response process in place and sufficient mechanisms to notify security breaches, and to share information during and after an incident.
15. Continuously monitoring the security state of the on-cloud hosted information systems to support on-going risk management decisions.

I.3. Information Access and Payment Initiation Service Providers

In addition to section [G.3], the entity has to ensure the security of financial transactions and messages either at-rest, in-use, or in-transit by considering at least the measures mentioned in section [G.4] and other parts of the framework, as well as related national and international regulations and standards mentioned in section [C]. In addition, the entity has to ensure:

1. Risk catalogs across all provided APIs are maintained and include all available capabilities of fraud detection, anti-money laundering, and data privacy. Catalogs should address what information that should be captured by third-party service providers (e.g. mobile phone IMEI or ESN and location) and then transferred to the entity to enable suspicious activities detection.
2. Roles and responsibilities required for responding to fraud and cyber cases and incidents must be clarified.
3. To increase the privacy and minimize the risk of fraud, users' actual identifiers should not be shared with third-party service providers. The entity should generate unidirectional, opaque and un-guessable subscriber identifier for each user to be used at a specific third-party service provider.
4. Communications between the third-party service providers and the entity has to be established over secured VPN tunnels. It is highly recommended to deploy IPSec with IKEv2 and certificate-based peer authentication.
5. Networking and routing mechanisms implemented by service providers should be inspected to ensure that they are not enabling network access and disclosing the entity's private network information among the connected participants and entities.
6. Third-party service providers have to be authenticated prior to consuming any provided API. It is highly recommended to use end-to-end mutual TLS 1.2 (or later) authentication with digital certificates issued by trusted CAs.
7. For user and client authentication:
    7.1. The entity has to utilize their existing mechanisms (more than relying on third-party mechanisms) to authenticate users, and provided credentials by at least two factors and before registering the consent. Refer to section [G.3] for acceptable authentication factors.
    7.2. Clients have to be authenticated at API level once the consent is registered, it's highly recommended to use OAuth 2.0 with OpenID Connect 1.0. Generated and processed tokens and assertions must be digitally signed by the private key of the entity, and verified by the third-party service provider, as well as encrypted asymmetrically using third-party service provider's public key.

8. User has to explicitly authorize the third-party service provider before granting access to user's hosted data or to initiating transaction on his/her behalf. It is highly recommended to use scopes and claims available in OAuth/OIDC to register consent.
9. Providing the user with all required facilities for revoking and withdrawing a granted consent at any time.

I.4. Identity, Credential Management and Federated Authentication

In addition to sections [G.3] and [I.1], and when the entity acts as a relying party on a third-party credential service provider and identity provider for identity services (i.e. enrollment and identity proofing, authentication, authorization and attribute assertion), the entity should ensure that the service is delivered with the assurance levels and controls that are expected by the entity for identification, authentication and federation. Accepted levels of assurance and controls should be determined based on risk assessment process, and guided by the international standards and best practices. Recommended sources are the latest published revisions of related **NIST** special publications.

In general, the entity should ensure the ability of the credential service provider and identity provider to:

Enrollment and Identity Proofing

1. Provide protection mechanisms no less than what mentioned in section [H.5].
2. Reduce the amount of PII vulnerable to unauthorized access or use through minimizing data collection, and collecting only the PII necessary to validate the existence of the claimed identity and associate the claimed identity to the applicant.
3. Provide explicit and effective notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory.
4. Provide the capability for granular administration of gathered PII, including alteration, deletion, and enabling selective use or disclosure of attributes.
5. Provide clear notice and obtaining user (subscriber) consent if the collected attributes are processed for purposes other than identity services.
6. Maintain whitelists of relying parties that are authorized to receive authentication and attributes without a runtime decision from the subscriber, as well as blacklists of relying parties that are not authorized to receive authentication or attributes even when requested by the subscriber. Identifying relying parties should be based on sufficiently unique identifiers depending on the federation protocol in use.
   For relying parties that are not on a whitelist or a blacklist; the identity provider has to ask for runtime authorization decision from the subscriber. Identity provider can remember a subscriber's decision to authorize a given relying party but with allowing the subscriber to revoke remembered access at any future time.
7. Provide effective mechanisms for redressing applicant complaints or problems arising from the identity proofing, and utilize simple and easy mechanisms for applicants to find and access.

Federated Authentication

1. Include the following metadata in the authentication assertions:
   - Random and non-guessable assertion unique identifier
   - Subscriber (subject) identifier
   - Identity provider identifier
   - Relying party identifier that is intended to consume this identifier
   - Attribute values and metadata
   - Issuing timestamp and expiration timestamp
2. Having information exchanged between relying party and identity provider digitally signed by identity provider's private key and verified by the relying party. It must also be sent over an authenticated and protected channel.
3. Implement back-channel presentation model (highly recommended) in which a subscriber is just given an assertion reference to be presented to the relying party (the entity). Assertion reference should not contain information about the subscriber and be resistant to tampering and fabrication. The relying party then presents the assertion reference to the identity provider, along with authentication of the relying party itself, to fetch the assertion.

   In cases where assertions pass through subscriber instrument (e.g. browser or mobile application); the assertion must be digitally signed by the identity provider's private key and verified by the relying party, as well as encrypted asymmetrically using the relying party's public key. Used digital certificates should be issued by a trusted CA among all the parties. It is highly recommended in such cases to deploy a mechanism depending on proving the subscriber's possession of a key referenced in the assertion (i.e. holder-of-key assertions) when being represented to the relying party more than depending on bearer assertion model.
4. Identity providers may build profiles of subscribers based in the processed transactions, but profile patterns should not be shared with any entity without explicit notice to the subscriber and obtaining consent.
5. Implement blinding technologies when the entity interacts with the identity provider(s) through a federation proxy (i.e. broker) to increase the level of data privacy and reduce the risk of revealing identifying information of the entities participating in the federation.

PART3 Crisis Management and Contingency Planning

J. Incident Management and Response Planning

J.1. Incident Management Process

The entity has to define and maintain an incident management process to ensure it has a set of procedures and actions needed to respond to and resolve incidents. The process should at least include:

1. Predefined procedures and actions of detecting, confirming and classifying incidents. This responsibility should be assigned to the Information Security Management. Criteria for detecting and confirming incidents should align with section [G.10].
2. Building a cyber incident response team that consists of the personnel and/or third-party individuals who will response to an incident. The structure of the team should consist of:
   2.1. An incident manager to ensure that all actions are tracked, documented and are well communicated as well as escalated when needed. This role should be assigned to the accountable manager of cybersecurity function.
   2.2. Core members would at least be:
   - Response team to perform technical response and recovery procedures. The members of this team can include:
     - IT, infrastructure staff, cybersecurity investigators and analysts with strong networking, log analysis, and forensics skills.
     - Partially or fully outsourced core members. Outsourcing arrangements must be in line with the controls mentioned in section [I].
   - Handling team to perform logistics, communications, coordination, and planning functions that are needed in order to resolve the incident.

   It is highly recommended to have two separated roles for leading response and handling teams.
   2.3. Extended members where needed, such as:
   - Business, HR, legal and risk departments, as well as public relations.
   - Disaster recovery and business continuity planning teams when there is a serious damage and outages.
   - Data privacy and protection teams.
3. Ensuring the continuous availability of required incident preparation items such as:
   - Data backup schedules.
   - Updated infrastructure and system architectural designs and documentations.
   - Updated Copies of all available contact information and service agreements.
   - Qualifications and skills of technical and security staff.

- Equipped central physical or virtual room for communication and coordination.
- Packet sniffing, protocol analyzers, as well as evidence acquisition and digital forensic investigation tools.
- Forensic and analysis workstations.
- Evidence gathering accessories.
- Updated disaster recovery and business continuity arrangements.

4. Documenting all procedures and actions of response, containment, recovery and after action review. This responsibility should be assigned to the Incident Manager.
5. Sharing of incident information and associated threat intelligence with FinCERT during different incident response phases.
6. Clearly definition of the threshold when the incident should be identified as a disaster. The threshold should consider the situations when the incident cannot be contained or causes severe damage.

J.2. Incident Handling, Response and Recovery

React and response

1. React and response procedures should be triggered quickly after detecting and confirming an incident. Procedures should ensure:
   1.1. Alert and notification list and alert messages should be prepared to notify key personnel. The list can include and not limited to:
      - Senior management and business owners.
      - CBJ and incident reporting organizations.
      - Law enforcement agencies if the incident violates civil or criminal laws and regulations.
      - Affected external partners.
      - Media.
      - ISPs for being ready for any expected action.
      - Support providers and software vendors and developers.
   1.2. Level of notification, who, and when to notify, based on the classification and the rated severity of the incident.
   1.3. Assignment of tasks and initiating documentation process of all proposed and taken actions

Containment

2. Incident response team should conduct a triage process and determine the appropriate and timely containment strategy to stop the incident impact, as well as to regain control of the affected assets. Criteria of determining the strategy should include:
   2.1. Potential damage and scope of the breach
   2.2. Determined service availability
   2.3. Estimated time duration and human resources needed to implement the strategy, and to provide a solution either a workaround solution or a permanent solution.
   2.4. Effectiveness of the strategy whether it provides partial containment or full containment
   2.5. Need of evidence preservation for legal or insurance purposes
   2.6. Assessment of raising new potential issues after containment (e.g. some attacks may cause additional damage when they are contained).
3. If applicable; incident responsible teams should work on identifying the attack source (i.e. host(s)) and validating the source IP address(es). This process could assist during containment process by which such information can be checked against incident databases and real-time blacklists to get more information about the APT that is launching the attack (if any), and look for the used tactics and techniques. Also, owners of attacking IP addresses can be contacted for further investigation.

4. An incident could be escalated to a disaster to trigger disaster recovery plan(s) if the predefined threshold was reached.

Eradication and Recovery

5. Incident response team has to assess the full extent of the damage and determine the scope of the breach on information assets CIA in order to determine systems and services recovery strategies and priorities.
6. The recovery process should at least include:
   6.1. Identifying root causes and remediating the vulnerabilities that allowed the incident to occur and spread.
   6.2. Identifying and reconfiguring the preventive controls that failed or missed from the firstly infected assets.
   6.3. Evaluation for monitoring capabilities to improve detection and reporting methods.
   6.4. Restoring data from backups if needed after ensuring the cleanliness of backup data.
   6.5. Compromised services and processes must be examined, cleaned, and then restored
   6.6. Continuously monitoring the systems and the network activity.
   6.7. Restoring the confidence of the organization's members.

Post-Incident Activity

7. Review response and handling actions during the incident, and identify areas where the incident response plan didn't work and propose improvements.
8. Determine what corrective actions should be taken to prevent similar incidents and what indicators to be monitored to detect such incidents.
9. Use incident's collected data into the risk assessment process, in order to measure the effectiveness of incident response team.

Forensic and Analysis

10. Forensic techniques can be integrated into incident response to:
    10.1. Preserve evidences for legal or insurance purposes. In this case, evidence acquisition, examination and custody management should follow the mandated procedures by the authorities.
    10.2. Analyze detected malware, determine attack tactics and determine the firstly infected asset.
11. Detailed logs for collected and preserved evidences must be maintained during incident response, and should include at least:
    - Evidence identifying information such as the location, hostname and IP address.
    - Contact information of the individual who performed the acquisition.
    - Evidence repository or store, and evidence acquisition time and date.

K. Incident Severity Rating and Sectoral Response

Classifying incidents through rating the severity should be performed at two levels; the organizational-level and the sectoral-level.

1. Organizational-level severity rating is performed by the entity to define the point at which the incident should be treated as a disaster, in addition to determine escalation procedures, as well as human resources and time durations to recover. The entity has to notify CBJ/FinCERT about the incident according to the following timelines:
   - Initial notification within 2 hours from confirming time.
   - After the closure of the incident for "Low" incidents.
   - Within 8 hours from confirming the incident and one time every two business days for "Medium" incidents.
   - Within 4 hours from confirming the incident and once a day for "High" incidents.
2. The entity should use the following impact category and severity rating matrix:

Incident Impact / Severity	Functional Impact	Information Impact			Recoverability Impact
	Service Disruption	**Data Privacy Breach**	**Data Integrity Breach**	**Proprietary Breach**	
Low	The entity can still provide all critical services to all users but with decreased efficiency	Sensitive information was accessed but not exfiltrated	Unclassified information was accessed or altered	The monetarized impact of fraud or theft of property can be absorbed by the entity	Time to recover is predictable
Medium	The entity has lost the ability to provide a critical service to a subset of users	Sensitive information was accessed and exfiltrated, and impacting less than 3% of the customer based	Low business-impacting information was accessed or altered	The monetarized impact of fraud or theft of property is little higher than what the entity can absorb	Time to recover is unpredictable, where additional resources and outside assistance are needed
High	The entity is no longer able to provide some critical services to any user	Sensitive information was accessed and exfiltrated, and impacting more than 3% of the customer based	High business-impacting information was accessed or altered	The monetarized impact of fraud or theft of property is more higher than what the entity can absorb	Recovery from the incident is not possible (e.g. PII data exfiltrated and posted publicly).

3. Sectoral-level severity rating is performed by CBJ/FinCERT to define the point at which a unified response should be coordinated to contain and recover from the incident.
   - For incidents that are classified as sectoral "Low", CBJ/FinCERT shall keep monitoring without coordinating unified action unless requested by any of the effected entities.
   - For incidents that are classified as sectoral "Medium" and "High", CBJ/FinCERT will manage unified response procedures to contain and recover from the incident.
4. CBJ/FinCERT shall use the following sectoral impact category and severity rating matrix:

Incident Impact / Severity	**Functional Impact**	**Information Impact**		
	Service Disruption	**Data Privacy Breach**	**Data Integrity Breach and Others**	**Proprietary Breach**
Low	One entity with organizational "high" incident OR 1 to 9 entities with organizational "medium" incident OR 1 to 15 entities with organizational "low" incident	One entity with organizational "high" incident OR 1 to 3 entities with organizational "medium" incident OR 1 to 10 entities with organizational "low" incident	One entity with organizational "high" incident OR 1 to 12 entities with organizational "medium" incident OR 1 to 18 entities with organizational "low" incident	One entity with organizational "high" incident OR 1 to 3 entities with organizational "medium" incident OR 1 to 10 entities with organizational "low" incident
Medium	Two entities with organizational "high" incident OR 10 to 15 entities with organizational "medium" incident OR 16 to 22 entities with organizational "low" incident	4 to 5 entities with organizational "medium" incident OR More than 10 entities with organizational "low" incident OR impacting between 3% to 10% from all financial consumers	Two entities with organizational "high" incident OR 12 to 20 entities with organizational "medium" incident OR 19 to 24 entities with organizational "low" incident	4 to 5 entities with organizational "medium" incident OR More than 10 entities with organizational "low" incident OR the total monetarized impact of fraud or theft of property is more than 10M JD
High	More than two entities with organizational "high" incident OR More than 15 entities with organizational "medium" incident OR More than 22 entities with organizational "low" incident	Two entities or more with organizational "high" incident OR More than 5 with organizational "medium" incident OR impacting more than 10% from all financial consumers	More than two entities with organizational "high" incident OR More than 20 entities with organizational "medium" incident	Two entities or more with organizational "high" incident OR More than 5 with organizational "medium" incident OR the total monetarized impact of fraud or theft of property is more than 20M JD

L. Disaster Recovery and Business Continuity Planning

The entity has to develop, maintain, implement, and communicate disaster recovery and business continuity policy and plans to identify the procedures and actions needed to manage a disruptive interruption and to restore or reestablish business processes and operations to acceptable levels.

1. Disaster recovery process should be managed and supervised directly by the senior management.
2. The disaster recovery and business continuity governance must be clearly defined, roles and responsibilities must be assigned, also related authorities and external stakeholders must be identified.
3. The entity should predefine availability and recovery objectives for business functions based on the criticality and sensitivity (i.e. BIA). Objectives should include at least:
   - Annual SLO
   - MAO, RTO and RPO
4. Availability and recovery objectives should be reflected into the architectural design of the systems and applications, as well as addressed by developing disaster recovery and business continuity plans that define:
   4.1. Scenarios of outages and service disruption caused by environmental, operational or cybersecurity incidents. Developed scenarios should consider the situations when primary sites are completely inaccessible.
   4.2. Procedures and techniques to achieve availability at the level of:
      - Data, whether in-site (i.e. mirroring) or over sites (i.e. replication), as well as data restoration. Deployed techniques should ensure the isolation of logical corruptions among the sites.
      - System service, either in-site (e.g. clustering for stateful applications, load balancing for stateless applications, etc.) or over sites (e.g. stretched clustering, global load balancing, etc.).
      - Service network accessibility by the consumers in a seamless manner.
   4.3. The entity has to establish alternative site(s) to reestablish critical business services and operations. The alternative site(s) could be based on either exclusive or shared use options. In both options, the alternative site(s) should be located in a physically separated secure location, and with the same level of cybersecurity controls that are implemented in the main site.
   4.4. Step-by-step procedures and guidelines of carrying out switchover/failover, as well as resuming operations to business-as-usual after resolving the incident. Also, procedures should define key resources in terms of people, involved third parties and service providers, contacts and communication channels, as well as technologies. Switching to the alternative site(s) procedures should consider scenarios of complete and unplanned outages of the primary site(s).

5. The entity should measure actual SLIs annually to ensure the compliance with predefined SLOs. Deviations should trigger an assessment, evaluation and remediation processes for the procedures and controls in place.
6. The entity should provide physically secure workspace(s) with pre-arranged seats to relocate the resources required to deliver the critical business processes. Workspace(s) should be designed to be activated independently from the primary site.
7. Tabletop, simulation and structured walkthrough exercises should be conducted on regular basis to validate disaster recovery and business continuity plans scenarios and procedures.
8. Disaster recovery and business continuity actual tests should be conducted at least annually, and upon major changes, for critical systems and services. Results of exercises and tests should be evaluated, documented and signed off by senior management.
9. If the entity relies on a third party service provider(s) for a critical business service(s), the entity should ensure that the service provider(s) maintain a business continuity plan that meets the entity recovery objectives.
10. Disaster recovery plans and procedures should include:
    10.1. Verifying personnel status.
    10.2. Preparing alert message and description, and executing alert list.
    10.3. Establishing disaster declaration and keep public informed.
    10.4. Communicating with relevant, internal and external stakeholders and parties.

PART4 Collaboration

FinCERT

Information Sharing

Sectoral Awareness

Meetings

FinCERT

FinCERT is a part of the National CERTs and will work in coordination with CBJ-regulated entities to boost the level of protection across the sector. Some activities at the national level will be funneled through the National CERT, while others related to financial sector will be carried-out by the FinCERT and briefings will be communicated to the National CERT.

FinCERT unit (i.e. FinCERU) has been created within CBJ organizational structure with the objective of mainly developing and maintaining cybersecurity frameworks and programs. In addition to handling cybersecurity incidents, and addressing intelligence information operations reported by the community.

FinCERT executive committee structure contains members of CBJ and the banking community. The main tasks of this committee is to review and revise the outputs and deliverables of FinCERT unit, overseeing the unit activities and KPIs and managing sector-wide crises.

Cybersecurity board is on the top of FinCERT structure, headed by H.E. the Governor of Central Bank of Jordan and joined by both CBJ deputy governors and a number of CEOs from the banking community. The board is responsible for providing upper management support and commitment, adoption of strategies and policies, being informed about sector-wide security posture and to set directions.

Roles and Responsibilities

FinCERT

FinCERT is responsible for developing, and implementing a cybersecurity road map which includes action plans resulting in programs and frameworks for cybersecurity. This also includes publishing advisories and actionable measures, monitoring and evaluating functions for the outcomes and deliverables, as well as developing an accreditation program for cybersecurity service providers (companies) dealing with the financial sector.

FinCERT is representing the sector and acting as a focal point in communicating and sharing intelligence information with related parties such as National Cybersecurity Center of Jordan, intelligence units and other national CERTs.

FinCERT is also responsible for following up institutional-level cyber incidents response, and managing sectoral-wide crises.

CBJ

CBJ is the regulatory authority for the financial sector in Jordan and responsible for issuing cybersecurity regulatory frameworks and perform compliance-check on the sector parties. All non-compliance and

deviation cases with cybersecurity programs, frameworks, action plans, policies, standards and procedures shall be reported to CBJ regulatory departments to take the proper actions.

Furthermore, CBJ is supervising the operation of the main components of payment infrastructure in Jordan. Therefore, CBJ shall have a role in the management of cyber incident response for the incidents that are targeting the payment infrastructure within the sector.

Banks and Financial Institutions

Banks and Financial institutions are responsible for applying cybersecurity programs, frameworks and measures, respond to cyber incidents and exchange incident information and threat intelligence with FinCERT. Financial institutions also have to follow the FinCERT published security, technical, operational and procedural standards and recommendations especially when dealing with 3rd-parties and outsourcing service providers. In addition, financial institutions have to work on increasing the security awareness levels of their clients and stakeholders.

Information Sharing

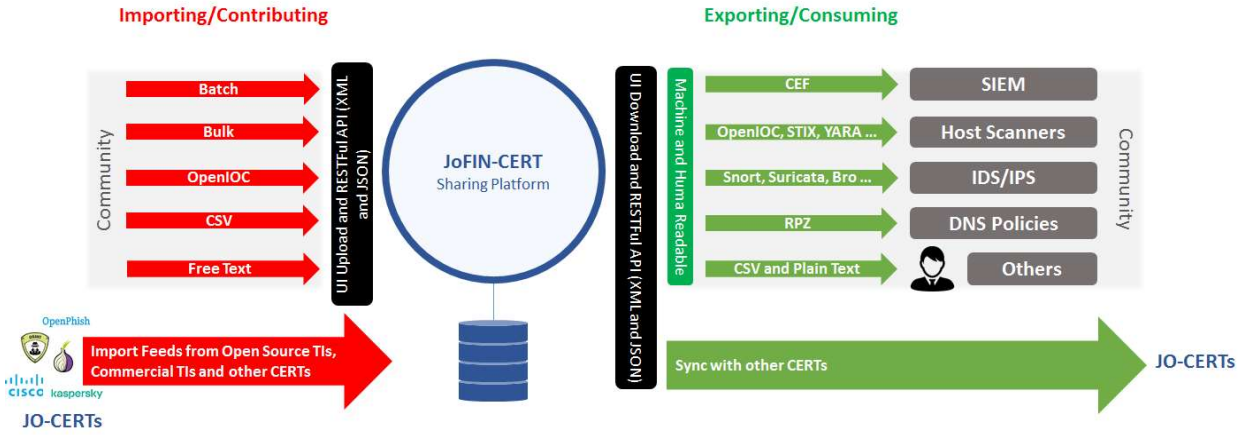


Figure 1 – Information Sharing

Sharing and exchanging information within the community about global and local incidents, threats and vulnerabilities will equip the community to become more resilient towards cyber incidents.

FinCERT shall manage the process of developing and federating the information-sharing platform, which is planned to be hosted at CBJ and accessible by all participating banks and financial institutions. Intelligence information shall be automatically fed and imported from different trusted public and private sources or be processed manually by participants. This allows all members to browse and instantly get an updated information of global and local incidents to enrich detective or preventive controls, and conduct necessary assessment of their protection levels against reported attack method. FinCERT shall perform daily analysis and further disseminate information.

Sectoral Awareness

FinCERT in cooperation with entities' accountable managers of cybersecurity function and well qualified 3rd-parties shall manage preparing awareness materials and conducting awareness and training sessions designated for different levels and roles of the employees.

Meetings

FinCERT will hold periodic meetings at least once every quarter or whenever necessary in the presence of entities' accountable managers of cybersecurity function or whoever needed. Additional meetings can be held when formally needed and requested.

Preparing meeting agenda will be done within ten business days prior to the meeting, and then distributed within two business days in advance, so that entities can prepare accordingly. Meeting minutes will be recorded by FinCERT representative, and distributed to the entities for review before finalizing.

PART5 Assessment

Cybersecurity Readiness Assessment

Maturity Model

The cybersecurity maturity level of each entity shall be benchmarked and measured according to the alignment of the current security state with the domains covered in this framework. The maturity model has six maturity levels, and focuses on people, policies and procedures in place, as well as existing technical solutions.

Based on the outcomes of the assessment process, a set of prioritized remediation action plans shall be developed and implemented to achieve the targeted maturity level.

Maturity Levels

Level 0	Complete absence of the control
Level 1	Compliance-driven objectives are achieved by practicing the control or the process, and basic expectations required or recommended by laws and regulators are available.
Level 2	The control or the process is formally identified and practiced with relative consistency, and characterized for a subset of the organization (e.g. project).
Level 3	• Risk-driven objectives are achieved by practicing the control or the process commensurate with the risk. • The control or the process is practiced consistently and formally identified by formal strategy and plans that define the consistent achievement across the organization.
Level 4	• Outcomes are measured and reported. Elicited indicators contribute to risk management process and continual improvement. • Majority of risk management processes are automated. • Cybersecurity practices and analytics are integrated across lines of business.
Level 5	Practiced control and process is subject to continuous improvement based on organizational changes and lessons learned internally and externally.

Organizational Assessment

By this framework; the assessment will consist of two parts:

Part 1: Profiling Entities

Each entity shall be profiled and classified based on the assessment of its risk profile. Assessing risk profile depends on measuring risk levels based on type, volume and complexity of the entity's operations within activities and services that are organized into five major categories:

1. Service Delivery Channels
2. Internet and Mobile Banking Services
3. Technologies and Connections
4. External Threats
5. Organizational Characteristics

Part 2: Assessing Maturity Level

Entity's maturity level shall be measured within each of the following five major domains:

Domain 1: Cybersecurity Governance and Management Controls

Domain 2: Cybersecurity Technical and Operational Controls

Domain 3: External Dependencies

Domain 4: Response and Recovery

Domain 5: Threat Intelligence and Collaboration

Each domain is composed of a collection of subdomains, where the subdomain is a grouping of related components and set of activities under each component.

Each activity is assigned a target maturity level, and the overall domain maturity level is calculated by considering the actual state of each activity.

As a result of assessing the risk profile of the entity and assessing the maturity level within each domain, the overall domains maturity levels should increase when risk levels rise. Depending on the results and determined target maturity levels, a gap analysis process should be conducted, and then remediation plans should be developed, prioritized and implemented within tolerated time frames.

Assessment tools are developed and delivered by FinCERT, self-applied by entities, and then reviewed by FinCERT. Face-to-face physical or virtual meetings could be conducted during FinCERT review.

Sectoral Assessment

Banks shall be weighted based on their impact on the national financial stability. The overall sector security position shall be calculated based on organizational assessment's results and tiers of banks. FinCERT shall publish the assessment criteria with more elaboration and clarification.

Control Assessment

To minimize the risk of false sense of security; an assessment framework shall be established for measuring the effectiveness and efficiency of the adopted controls in real life scenarios, to ensure that these controls are achieving their objectives as expected. The framework aims to assess the defenses and the response of the entities to a range of external attacks including people risks.

Control assessment process shall be implemented by FinCERT either by internal resources or by engaging 3rd-parties, and shall be conducted after ensuring achieving the targeted maturity levels on the national financial sector.

Review and Continual Improvement

Improvement is a continuous process as cyber threats and vulnerabilities evolve rapidly, the composition of the financial sector also changes over time, as new types of entities, products, and/or services emerge, and third-party service providers are increasingly relied upon. FinCERT shall be reviewing cybersecurity framework and ensuing documents and tools biennial.

Entities also can request update on the framework by applying a formal application approved by its information security management and the cybersecurity committee.

Communication and Reporting

Entities shall name their representatives to communicate and report with FinCERT in order to implement this framework. Representatives have to include at least the Head of Information Security Management and the head of Information Technology. Maximum number of representatives from each entity could be four persons.

Exemption

The entity may acquire an exemption from one or more of the aforementioned controls during the implementation of the framework. The exemption request should be justified and formally sent to the CBJ/FinCERT to be evaluated and assessed.

Contact Information

All communications from the representatives of member entities should be addressed to fincert@cbj.gov.jo.

APPENDIX A Acronyms

COMMON ABBREVIATIONS

Abbreviation	Explanation
AES	Advanced Encryption Security
AI	Artificial Intelligence
API	Application Programmable Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ATM	Automated Teller Machine
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BYOD	Bring Your Own Device
CA	Certificate Authority
CAB	Change Advisory Board
CERT	Computer Emergency Response Team
CHD	Cardholder Data
CIA	Confidentiality, Integrity and Availability
CMMI	Capability Maturity Model Integration
CPE	Common Platform Enumeration
CRUD	Create, Read, Update, Delete
CVE	Common Vulnerabilities and Exposures
CSA	Cloud Security Alliance
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DevOps	Development and Operations
DH	Diffie Hellman
DHCP	Dynamic Host Control Protocol
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting & Conformance
DMZ	demilitarized zone
DNS	Domain Name System
DoS	Denial of Service
DREAD	Damage, Reproducibility, Exploitability, Affected Users, Discoverability
DSA	Digital Signature Algorithm
ECC RAM	Error correction code Random Access Memory
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm

EMV	Europay, MasterCard and Visa
ESN	Electronic Serial Number
EV	Extended Validation
FinCERT	Financial Cyber Emergency Response Team
FTP	File Transfer Protocol
GSM	Global System for Mobile Communications
HMAC	Hash-based Message Authentication Code
HTTP/S	Hypertext Transfer Protocol/Secure
ID	Identifier
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IoC	Indicator of Compromise
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol v4
IPv6	Internet Protocol v6
ISO	International Standards Organization
IT	Information Technology
KRI	Key Risk Indicator
L2	Layer 2 (From network OSL model)
L3	Layer 3 (From network OSL model)
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MAO	Maximum Acceptable Outage
MDM	Mobile Device Management
MiTM	Man-in-The-Middle
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
ML	Machine Learning
NDA	Non-Disclosure Agreement
NFC	Near-Field Communication
NFS	Network File System
NVD	National Vulnerability Database
OAuth	Open Authorization
OCR	Optical Character Recognition
OIDC	OpenID Connect
OS	Operating System
OSINT	Open Source Intelligence
OTP	One-Time Password
OVAL	Open Vulnerability and Assessment Language

OWASP	Open Web Application Security Project
PASTA	Process for Attack Simulation and Threat Analysis
PCI DSS	Payment Card Industry Data Security Standard
PCI PA-DSS	Payment Card Industry Payment Application Data Security Standard
PCI PTS	Payment Card Industry PIN Transaction Security
PII	Personal Identifiable Information
PIN	Personal Identification Number
PoI	Point of Interaction
PoS	Point of Sale
PTR	DNS Pointer Record
QR	Quick Response
RACI	Responsible, Accountable, Consulted and Informed
RADIUS	Remote Authentication Dial-in User Service
RDBMS	Relational Database Management System
RPC	Remote Procedural Call
RPO	Recovery Point Objective
RSA	Rivest–Shamir–Adleman
RTO	Recovery Time Objective
S/MIME	Secure/ Multipurpose Internet Mail Extensions
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SCAP	Security Content Automation Protocol
SCP	Secure Copy Protocol
SHA	Secure Hashing Algorithm
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLI	Service Level Indicator
SLO	Service Level Objective
SMB	Server Message Block
SMS	Sort Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPF	Sender Policy Framework
SQL	Structured Query Language
SSID	Service Set Identifier
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure
SWIFT CSP	Swift Customer Security Program
TCP	Transmission Control Protocol
TKC	Threat Kill Cycle

TLS	Transport Layer Security
USSD	Unstructured Supplementary Service Data
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
ZTA	Zero Trust Architecture

APPENDIX B Framework Summary

#	Domain	#	Control			Description
PART1 Cybersecurity Governance and Management Controls						
A	Cybersecurity Oversight and Governance	1	Roles and Responsibilities			Information security roles and responsibilities are identified and mapped with internal roles
		2	Strategy and Policy			Information security strategy, policy and procedures are established and authorized
B	Cyber Risk Management	1	Cyber Risk Management Process			Risk management processes are established and risk tolerance is stated clearly
		2	Cyber Risk Assessment	2.1	Information Classification	Information assets are classified and handled based on the classifications
				2.2	Asset and Activities Prioritization	Assets, resources and business processes are valuated, weighted and prioritized based on criticality and sensitivity
				2.3	Risk Identification	Assets, threats and vulnerabilities are identified
		3	Cyber Risk Analysis and Evaluation			Risks business impacts and likelihoods are identified and risks are evaluated
		4	Cyber Risk Treatment			Risk responses and mitigation controls are identified and prioritized
		5	Cyber Risk Monitoring and Review			Risk metrics are identified and monitored and risk registers are reviewed periodically and after changes, and altered accordingly
		6	Project Management			Projects go through information security assessment
		7	Cyber Risk Insurance			Cyber risks are covered by insurance
C	Cybersecurity Compliance	1	National Regulations and Standards			All relevant national legislative, standards, regulatory or contractual requirements related to security are identified and considered
		2	International Regulations and Standards			All relevant international and industry legislative, standards, regulatory or contractual requirements related to security are identified and considered
D	Cybersecurity Audit	1	Internal Audit			Audit on information systems is conducted by in-house team
		2	External Audit			Audit on information systems is conducted by external bodies
E	Human Resources	1	Human Resources Security			Ensure protection of organization's information assets and interests during hiring, changing and terminating employees and contractors

		2	Awareness and Training			Employees and contractors are aware of information security responsibilities
PART2 Cybersecurity Technical and Operational Controls						
F	Asset Identification	1	Identifying Information Assets			Information assets are identified and inventoried.
		2	Identifying People			Personnel that enable the organization to achieve business purposes with their relative importance to organizational objectives and the organization's risk strategy are identified.
		3	Identifying Business Processes and Activities			Business processes and activities, dependencies and critical functions for delivery of critical services and resilience requirements to support delivery of critical services for all operating states are identified and established.
G	Prevention and Detection	1	Physical Assets Security	1.1	Secure Access	Secure areas, locations, rooms and offices are established and identified
						Assets off-premises are protected and secured by considering different risks
						Unattended assets are protected and secured by considering different risks
						Operating procedures for papers, removable storage media and a screen policy are adopted and communicated
						Data cables are protected against interception, interference or damage
				1.2	Operation Physical Environment Protection	Operation physical environment is protected against natural disasters, malicious attack and accidents
				1.3	Continuous Monitoring	Environmental and security continuous monitoring and alerting are established
		2	Resiliency by Design	2.1	Development, Test and Production Environments	Development, test and production environments are segregated and zoned, and measures to secure environments are implemented
				2.2	Secure Development Lifecycle	Secure development lifecycle is established and implemented
				2.3	Secure Coding	Secure coding methodology is developed and implemented
				2.4	Threat Modeling	Threat modeling approach for developed and implemented systems is established and communicated
		3	Identity Management, Authentication	3.1	Identity Management	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

			and Access Control	3.2	Authentication	Access tokens, authentication keys, secrets and passwords are assigned, controlled and managed
						Users, devices, and services are multifactor authenticated based on the criticality and sensitivity of the information assets accessed
				3.3	Access Rights Management	Authorizations and access rights are controlled, managed and reviewed
				3.4	Logical Access	Wired and wireless network access and access to network services and Internet is controlled, managed and audited
						Access to platforms and operating systems is controlled, managed and audited
						Access to systems and applications is controlled, managed and audited
						Administration and management access is controlled, managed and audited
				3.5	Network Segmentation and Zoning	System services are segmented and isolated based on the roles
						Client network is segmented based on the roles and business needs
		4	Data Protection	4.1	Data Confidentiality	Data confidentiality at rest is protected
						Data confidentiality during exchange is protected
				4.2	Data Integrity	Data integrity at rest is protected
						Data integrity during exchange is protected
						Integrity checking means and mechanisms are implemented to verify the integrity of information and assets
				4.3	Authenticity	Data and data source are verified
				4.4	Repudiation	Data communication is protected to ensure non-repudiation
				4.5	Data Privacy	Protecting data privacy procedures and mechanisms are implemented
				4.6	Data Leak	Data is protected from being leaked
				4.7	Email Security	Email security measures are implemented
				4.8	Removable Media	A process to manage removable media, media disposing and media transportation is in place
		5	Information Protection	5.1	Configuration Management	A baseline configuration of information assets is created and maintained
				5.2	Change Management	Configuration change process is controlled and managed

				5.3	Patch and Vulnerability Management	A process to manage patching systems is defined and managed
				5.4	Capacity and Performance Management	Adequate infrastructure capacity to ensure productivity is maintained
				5.5	Backup and Restoration Management	Backups of information are conducted, maintained, and tested
				5.6	Data Retention and Destruction	A defined process to manage data retention, reuse and destroy
		6	Infrastructure and Network Security	6.1	Protection Technologies	Technical security solutions are managed to ensure the security of systems and information assets
				6.2	System and Application Hardening	Systems, applications and assets are hardened
		7	Remote Access	7.1	Remote User Access	Remote users teleworkers connections are securely established
				7.2	Site-to-Site Access	Connections among branches and partner networks are securely established
		8	Cryptograph	8.1	Key Management	Controls to protect cryptographic Keys are developed and implemented through their lifecycle
				8.2	Mechanisms	Cryptographic technologies and techniques or correctly selected and management
		9	Logical Monitoring and Detecting	9.1	Network Monitoring	Network flows among information assets are monitored and analyzed
						Network usage is monitored and analyzed
				9.2	Personnel, Device and Service Activities Monitoring	Personnel, device and service activities are monitored and logged to prevent unauthorized access and covert connections
				9.3	Detecting Malicious Activity	Processes to detect and prevent malware and malicious activities are in place
				9.4	Detecting Unauthorized Code Installation or Injection	Processes to detect installation of software and code injection on operational systems and applications are in place
				9.5	Vulnerability Scanning and Penetration Testing	Vulnerability scanning and penetration testing processes are implemented and managed
		10	Event data and Evidences	10.1	Clock Synchronization	All systems clocks are synchronized
				10.2	Events Sources, Collection and Tracing	Events sources are specified and events are collected into a centralized repository

				10.3	Analysis and Correlation	Analysis and correlation rules are implemented and maintained
				10.4	Alerting	A process to manage rating events and alert is implemented and managed
		11	Cyber Threat Management			Cyber threat intelligence is received and processed
		12	Mobile Devices	12.1	BYOD	Security measures to manage the risks introduced by BYOD are adopted and implemented
				12.2	Portable Devices	Security measures to manage the risks introduced by portable devices are adopted and implemented
		13	Maintenance			Maintenance and repairs of information assets and system components are performed
H	Electronic Services	1	Financial Transaction			Financial and messaging networks are monitored and secured to prevent fraudulent and malicious activities and unauthorized access
		2	Service Delivery	2.1	Online Banking	Measures and controls to secure exchanged information and payments initiated by mobile and web applications from cyber risks and malicious activities are implemented and maintained
				2.2	Self-Service Machines and PoS/POI	Measures and controls to secure exchanged information and payments initiated by self-service machines from cyber risks and malicious activities are implemented and maintained
				2.3	Contactless Payments	Measures and controls to secure exchanged information and payments initiated by harnessing NFC and QR contactless technology from cyber risks and malicious activities are implemented and maintained
				2.6	Other Service Channels	Measures and controls to secure exchanged information and payments initiated by email, fax, texting applications, phone calls and physical mail from cyber risks and malicious activities are implemented and maintained
		3	Card Payment Operations			Measures and controls to secure payment card transactions and information from cyber risks and malicious activities are implemented and maintained
		4	Customer Notifications			Secure costumer notification and awareness programs are established

		5	Digital Onboarding	Measures and controls to secure digital onboarding process are implemented and maintained
I	Third-Parties	1	Contractors and Vendors	Processes to identify, assess, manage and mitigate supply chains, contractors and vendors risks are established and implemented
		2	Cloud Security	Processes to identify, assess, manage and mitigate cloud service providers risks are established and implemented
		3	Information Access and Payment Initiation Service Providers	Processes to identify, assess, manage and mitigate 3rd-party account information access and payment initiation service providers are established and implemented
		4	Identity and Credential Management and Federated Authentication	Processes to identify, assess, manage and mitigate credential service providers and identity providers risks are established and implemented
PART3 Crisis Management and Contingency Planning				
J	Incident Management and Response Planning	1	Incident Management Process	Incident management processes and responsibilities are clearly identified
		2	Incident Response, Handling and Recovery	Response processes and procedures are planned, tested and maintained, with coordination with internal and external stakeholders.
K	Incident Severity Rating			Incident alert thresholds are established
L	Disaster Recovery and Business Continuity			Resilience business requirements to support delivery of critical services

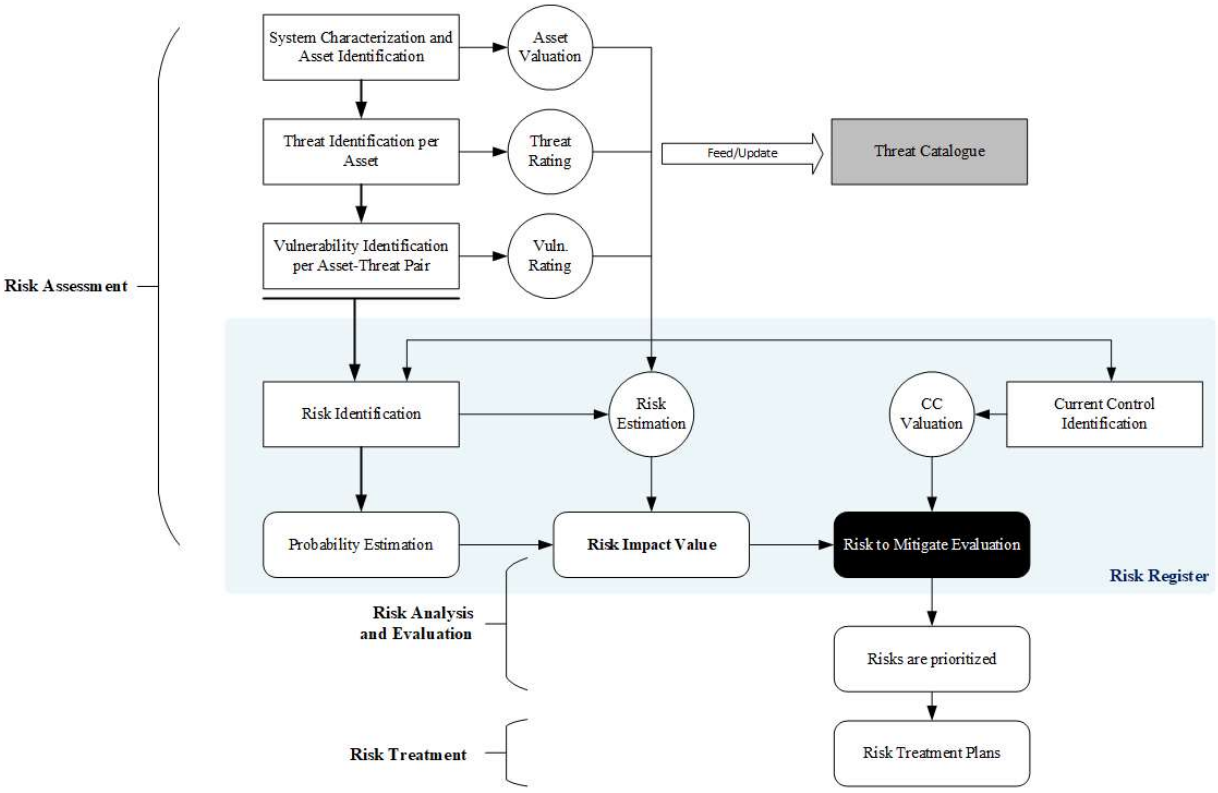
APPENDIX C Information Classification – Suggested Model

Data and information should be classified at least into four categories: public, internal use, secret and top secret based on the consequences of losing the confidentiality.

Attribute / Impact	Loss of Confidentiality		Classification
Financial Impact	*[Impact Quantitative Value]*		*Public, Internal Use, Secret, or Top Secret*
Legal Impact			
Operational Impact			
Reputational Impact			
	Quantitative Value : N/A : Low : Moderate : High	**Classification** : Public : Internal Use : Secret : Top Secret	**Final Classification**	***Most Restricted Class***

APPENDIX D Cyber Risk Management – Suggested Model

The diagram below illustrates the methodology of the suggested cyber risk management process



1. Risk Assessment

1.1 Asset Valuation

Asset valuation and weighting should consider **the sensitivity and criticality of the stored and processed data and information, and its relative importance to achieve business objectives**. Rating impacts can be quantitatively and/or semi-quantitatively.

Attribute / Impact	Weight	Loss of Confidentiality	Loss of Integrity	Loss of Availability	Weighted Asset Values
Financial Impact	W_F	*[Impact Rate]*			*Financial Impact =* $W_F * \sum[Impact\ Rates]$
Legal Impact	W_L				*Legal Impact =* $W_L * \sum[Impact\ Rates]$
Operational Impact	W_O				*Operational Impact =* $W_O * \sum[Impact\ Rates]$
Reputational Impact	W_R				*Reputational Impact =* $W_R * \sum[Impact\ Rates]$
W: 0 → 1 Impact Rate: 0 → 100					**Total Value of Asset**	$\frac{\sum[\boldsymbol{Impacts}]}{\mathbf{120}}$

Grading "Total Value of Assets" can follow the formula below:

Total Asset Value	Grade	Rate
0 ≤ value < 2	Very Low	1
2 ≤ value < 4	Low	2
4 ≤ value < 6	Medium	3
6 ≤ value < 8	High	4
8 ≤ value < 10	Very High	5

1.2 Threat Rating

Each threat should be rated based on the potential impact in terms of the caused financial loss, legal loss, operational loss, reputational loss, as well as human resources loss. Threats can be categorized into natural, environmental, or human acts whether deliberate or unintentional.

	Rate
Human Impact	Low (1), Very Low (2), Medium (3), High (4), Very High (5)
Financial Impact	
Legal Impact	
Operational Impact	
Reputational Impact	
Final Impact Rate	**The highest rate value**

For deliberate human acts specifically; the following factors can be included in the rating process plus to the potential impact of the identified threat:

1. Repeatability in the industry and the market.
2. Capabilities required by the actor to launch the attack against the entity in terms of financial, time and human resources as well as the level of needed skills and knowledge.
3. Potential gain and the ease of liquidating the stolen assets for financially motivated threats.
4. Discoverability of the attack considering the technical and business controls and operations, complexity of the market, and the level of the oversight.

Deliberate human acts grading can follow the formula below:

Factor	**Rating**	
Impact	1 → 3	Low, Very Low = 1 Medium = 2 High, Very High = 3
Repeatability	1 → 3	
Capabilities	1 → 3	
Gain	1 → 3	
Discoverability	1 → 3	
Threat Rate	$\frac{\sum[\boldsymbol{Rates}]}{\mathbf{5}}$	

The severity of the threat can be graded using the levels listed below:

Rate	Grade
1	Very Low
2	Low
3	Medium
4	High
5	Very High

1.3 Vulnerability Rating

Generally, vulnerabilities can be rated by considering two factors:

Factor 1 Susceptibility to exploit.

Susceptibility is a measurement of the efforts and resources required to exploit the vulnerability. The rate can be expressed semi-quantitatively in terms of:

Rate	Grade
1	Low
2	Medium
3	High

Factor 2 Exposure level of the vulnerability.

Exposure level is a measurement of potential exposure of the vulnerability to a threat event, considering whether the vulnerability can be tightly contained, affects multiple components or affects the majority of components. The rate can be expressed semi-quantitatively in terms of:

Rate	Grade
1	Low
2	Medium
3	High

The severity of the vulnerability can be graded using the formula below:

		Susceptibility		
		Low	**Medium**	**High**
Exposure	**Low**	Very Low (1)	Low (2)	Medium (3)
	Medium	Low (2)	Medium (3)	High (4)
	High	Medium (3)	High (4)	Very High (5)

NOTE: CVSS 3.1 can be used for rating and scoring technical vulnerabilities.

1.4 Risk Estimation

Vulnerability that could be exploited by an identified threat constitute an identified risk.

Potential identified risk value = vulnerability rate x threat rate x total asset value.

1.5 Risk Probability

Likelihood or probability of occurrence of the risk could be expressed semi-quantitatively based on the frequency of occurrence and the last occurrence seen.

The likelihood of occurrence for consequences could also be considered to calculate the total likelihood value:

Value of Probability	Description
1	Never happened (has not happened in the past three years)
2	Rare (happens once in year)
3	Periodic (happens once in a quarter)
4	Regular (takes place once in a fortnight)
5	Frequent (happens once in a week)

2. Risk Analysis and Evaluation

The risk impact value can be calculated by the following formula:

Risk impact value = potential identified risk value x risk probability.

To calculate the mitigated risk. Adequacy and values of current controls should be defined based on the level of protection that the controls provide for the asset CIA. Values can be defined quantitatively:

Grade	Value	Description
None	0	No control implemented
Low	1	Low level of implementation for the asset
Medium	2	Intermediary level of practicability for the asset
High	3	Strong level achievability for the asset

The total value of the current controls is the summation of C-value, I-value and A-value

Mitigated risk can be calculated by the following formula:

Mitigated risk = risk impact value / (current control value * accuracy of the assumption [%])

Based on mitigated values; risks should be ranked, ordered and then prioritized

Risk Levels Determination

Acceptable and tolerable risk levels should be clearly determined based on the values of assets, defined risk appetite as well as the risks probabilities.

The rates of threats and vulnerabilities, by which risks are introduced, should be clearly defined in the risk appetite statement in a context of what to be accepted and what to be tolerated.

Example:

Depending on defined risk appetite:

- The acceptable risk level is the highest total asset value (5), low threat rate (2), low vulnerability rate (2), and the highest probability (5), then (100) is the acceptable risk level.
- The tolerable risk level is the highest total asset value (5), medium threat rate (3), medium vulnerability rate (3), and the highest probability (5), then (225) is the tolerable risk level.

Results:

Risks below (100) can be accepted.

Risks between (100) and (255) need to be mitigated.

Risks above (255) are intolerable and could be avoided or transferred.

APPENDIX E Technical Vulnerability Management – Suggested Model

Scope of the model

The technical security vulnerabilities that can be identified by CVE feeds, vendor advisories and by the entity's technical teams, and affect the components below:

1. Firmware, Operating Systems and drivers
2. Middleware
3. Desktop and server applications
4. Relational Database Management Systems
5. Network Appliances

CVSS 3.1 scoring system can be adopted. Characteristics in CVSS are described through a set of metrics related to the vulnerabilities (Base), exploitability status (Temporal), and the organization (Environmental).

Software asset inventory should include CPEs (Common Platform Enumeration). CPE is a structured naming scheme released by NIST for IT systems, software, and packages. Each CPE has its related identified CVEs.

Roles and Responsibilities

Four main roles are participating in vulnerability management process:

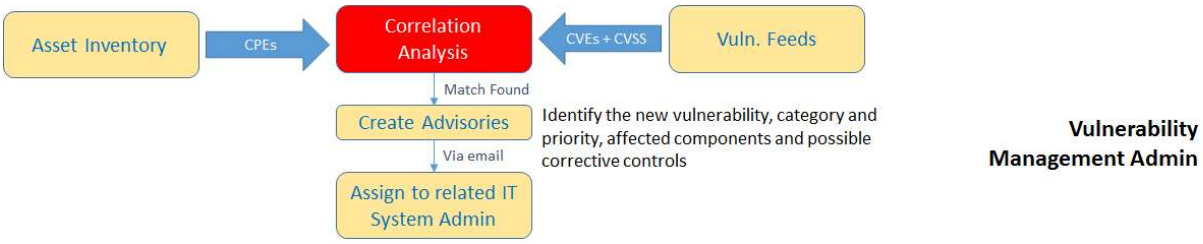
Role	Responsibilities
Vulnerability Management Admin (VMA)	1. Periodic monitoring for newly identified vulnerabilities and possible corrective controls. 2. Report newly identified vulnerabilities to IT system admins in form of advisories 3. Periodic reports for vulnerability management process
IT System Admin	Identify and apply the corrective controls with respecting the reported score of the vulnerabilities
Change Manager	Management of changes to be implemented on components affected by vulnerabilities and for the assessment of any conflicts with other concurrent activities
Business Owner	Ensure the success of applying corrective controls with no negative impact on business applications and processes

Workflow

1. Identifying New Vulnerabilities

Methods of identifying technical security vulnerabilities could be:

Method 1: CPE-to-CVE correlation analysis



- Correlation process can be done on a weekly basis by VMA.
- Possible corrective controls are defined based on CVE and related software vendor recommendations.

Method 2: Vendor advisory

VMA may receive advisories from vendors and external partners through trusted channels. Trusted channels could be:

1. Human intervention channels:
   - Pre-defined trusted email address
   - Trusted vendor portal
2. Trusted vendor automatic update services

For advisories received through email and downloaded from portals; VMA identify the vulnerability, categorize it, determine affected components, identify possible corrective controls, and then assign it to the related system admin(s). VMA has to build trust list for emails and portals delivering advisories. Portals must be checked on daily basis.

Update feeds from vendor update services may not have direct intervention from VMA.

Method 3: Technical Teams' Findings

Any finding reported by technical teams and controls must be reported directly to VMA to identify the vulnerability, categorize it, determine affected components, identify possible corrective controls, and then assign it to the related system admin(s).

2. Categorizing and Prioritizing Vulnerabilities

Categorizing and prioritizing vulnerabilities can be determined based on CVSS 3.1 (Base and Temporal) score, as well as the role and position of the affected components:

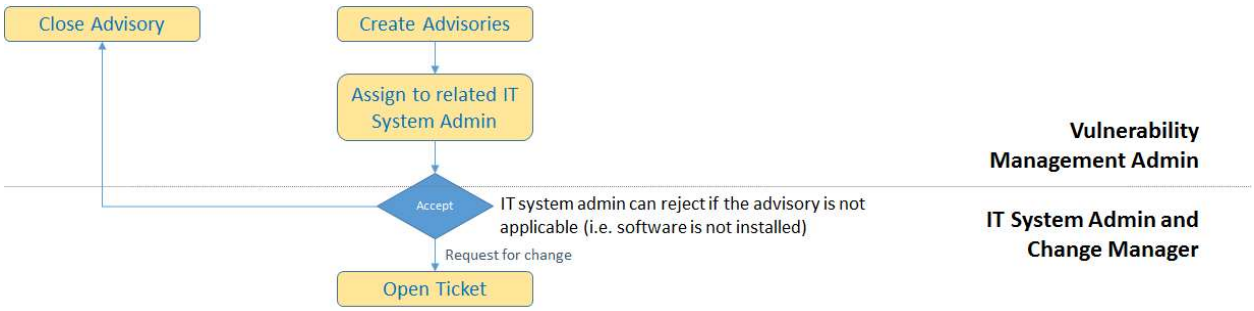
Affected Component	CVSS 3.1 (Base and Temporal) Score			
	Critical	High	Medium	Low
Internet-facing	5	4	3	3
Business critical system	4	3	2	2
Personal Computer	4	3	2	2
Non Internet-facing	3	3	2	1
Network Appliance	3	3	2	1

3. Remediation Plan

For CPE-to-CVE correlation analysis outputs, vendor advisories through human intervention channels, and technical teams' findings:

Assigned IT system admin can reject the advisory if it's not applicable, and rescore and re-categorize the vulnerability based on the controls on the ground. If it is accepted; the admin should identify the corrective controls to be applied and then initiates change management process. Corrective controls could be temporal or definitive.

Results and proper justifications should be sent back to VMA to be approved or re-advised.



Remediation plans could respect categories and priorities of vulnerabilities as below:

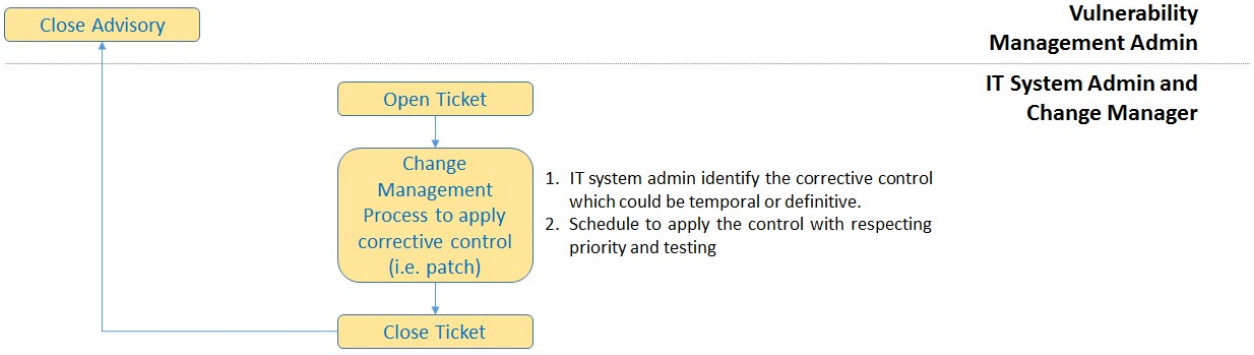
Category/Priority	Days to test if applicable	Overall days to treat
5	3 days	8 days
4	5 days	15 days
3	10 days	30 days
2	10 days	60 days
1	20 days	90 days

For findings from trusted vendor automatic update services:

1. Automatic push and automatic/manual installation for all categories of security vulnerabilities to:
   - Sample of client computers from different departments
   - Test instances
   - DR instances in case of not having test environment
   - One of production instances in case of neither having test nor DR environments.
2. Automatic push and automatic installation on all client computers after three working days from the successful installation and testing on the sample.
3. Automatic/manual push and manual installation on production systems after five working days from the successful installation and testing on Test/DR environment.

4. Execution

Execution can go through normal change management process.



If the proposed corrective control negatively affects business applications and processes, then IT system admin, business owner and VMA should define a compensating control, if no such control; risk assessment process should be triggered.

5. Closing

VMA is responsible for closing all advisories and report vulnerability management process periodically.