No. 26/1/1/1984

Date:6/2/2018

Central Bank of Jordan

Instructions of Cyber Risks Resilience

List of Contents

Chapter One

Attribution, Scope of Application and Definitions

Article (1):

These instructions are issued pursuant to the provisions of Article (4/ B/ 3 and 4) and Articles (50/ C, 65/ B) of the Central Bank of Jordan Law No. (23) of year 1971 and its amendments, Article (99/ B) of the Banking Law No. 28 of year 2000 and its amendments and Article (22/ B) of the Electronic Transactions Law No. (15) of year 2015 and its amendments, and shall be effective twelve months after issuance, unless specified otherwise.

Article (2):

These instructions shall be called "Instructions of Cyber Risks Resilience".

Article (3):

a. These instructions shall apply to all licensed banks, financial institutions, credit Bureaus, and microfinance companies that are under the oversight and supervision of the Central Bank of Jordan.

b. The branches of foreign banks operating in the Kingdom shall comply with these instructions as applicable, or comply with the governance and management of information and its related technology guide and policies issued by the parent bank, or the supervisory authority in their mother country, whichever is more likely to achieve the objectives of these instructions and in case the instructions that issued by the parent bank, or the supervisory authority in the parent country are more likely to achieve the objectives of these instructions the branch shall submit what verify this to the Central Bank, taking into account that there is no contradiction with the legislations in force in the Kingdom; wherever any contradiction occurs, the branch shall notify the Central Bank and the parent company about this contradiction and provide the necessary clarification to it, and obtain the Central Bank's approval regarding the procedures designated to address this contradiction.

Article (4):

The Bank when applying these instructions shall consider the provisions of the governance and management of information and its related technology Instructions No. (65/2016) dated 25/10/2016, especially what is related to the information technology risks and security management, and shall be read with it in an integrated manner. The financial institution, the credit bureau, and the microfinance company shall consider the implementation of the referred instructions to the extent that meet and complies with these instructions.

Article (5):

The following words and terms shall have the meanings assigned to each hereunder wherever mentioned in these Instructions unless the context indicated otherwise:

Financial Institution	:	Any public shareholding company or private shareholding company licensed to practice payment services or managing and operating electronic payment systems.
Credit Bureau	:	A Company licensed in accordance with the provisions of the Credit Information Law No. (15) of 2010 and the bylaw issued pursuant thereto.
Microfinance Company	:	A financial company that practice microfinance activities and licensed according to the provisions of the Microfinance companies Bylaw No. (5) of 2015.
The Company	:	The bank, the Islamic bank, the financial institution, the credit bureau or the microfinance company.
The Board	:	The company's board of directors and the like.
Executive Management	:	Includes the company's general manager / the regional manager, the deputy general manager/ deputy regional manager, the assistant general manager/ assistant regional manager, financial manager, operations manager, risk management manager, treasury (investment) manager and the compliance manager. In addition to any employee in the company who has an executive authority equivalent to the authorities of

those managers and is directly related to the general manager.

The information and communication technology (ICT) environment : It is a set of computer hardware equipment for internal networks, external networks, main servers, associated software, and all its supporting devices at the company's main and disaster recovery sites.

Information : Any oral or documented data, or any records, statistics, or any written, photocopied, recorded documents whether stored electronically, or in any other manner deemed to be significant to the Company.

Data : Raw facts that can be illustrated by letters, symbols and numbers which can represent people, things or events.

Information Assets : Any electronic or non-electronic information and files, hardware, storage media, software or any of the ICT environment components related to the company's business.

Cyberspace : A virtual environment consisting of the interaction of persons, software and services on the internet through associated hardware and technology networks.

Cyber Attack : Any attempt to destroy, expose, alter, impede, steal, or attempt to exploit vulnerabilities or illicitly access to the company's information assets within the cyberspace.

Cyber Resilience : The company's ability to anticipate , withstand, contain, and rapidly recover from a cyber attack.

Cyber Security : Preserve the confidentiality, the integrity, and the availability of the company's information and information assets within the cyberspace from any cyber threat through a set of means, policies, instructions and best practices thereon.

Cyber Threat : An incident or event that is likely to exploit (intentionally or unintentionally) one or more of the vulnerabilities in the company's ICT environment affecting the company’s cybersecurity.

Cyber Event : Any incident indicating the existence of a cyber threat to the company's ICT environment.

Cyber Risk : The combination of the probability of a cyber event occurring within the realm of a company’s information assets, and the consequences of that event on the company.

Cyber Governance : Arrangements a company puts in place to develop, implement and review its approach to manage the cyber risks.

Data Governance : The process of managing the availability, security, accessibility, and integrity of the data used in the company.

Malicious Code : Harmful software or files, which encompasses functions that have potential to adversely affect, directly or indirectly, the company’s ICT environment.

Protection : Implementation of appropriate measures, controls, and safeguards to enable reliable delivery of the company’s services and business.

Detection : Implement the appropriate controls and procedures in order to identify the occurrence of a cyber event immediately.

Response : Implement the appropriate controls and procedures to contain the cyber event upon detection.

Restore : The retrieval of information stored on backup media when the original information is disrupted or lost, or if it is required after a certain period to restore the company's business.

Recovery : A set of actions taken and followed to recommence the company's business to normal conditions, and reactivate the technology resources used to run the company's operations as it was before the event.

Vulnerabilities : A defect or lack of protection controls used in any of the ICT environment components related to the company's business, that can be exploited in hacking and cyber attacks.

Access Control : Rules and mechanisms used to allow only authorized persons to use and access the information assets in accordance with their responsibilities in the company.

Privileges : The level of authorities granted to users to access and use any of the components of the company's ICT environment.

Change Management : Manage, control and document any changes made to any of the company's ICT environment components, or any change in the procedures established in the company by the parties authorized to approve.

Information Classification : Determine the appropriate level of sensitivity of information created, altered, transferred, modified, or stored in any media, and by any available techniques, considering the risks of unauthorized access and illicit use of such information.

Confidentiality : Protect information against unauthorized access, dissemination, disclosure and illicit use.

Availability : The possibility of using and accessing the company’s information and systems, and retrieving them upon request.

Integrity : Accuracy, plenitude and soundness of information, information systems, or any part thereof and verify that there has been no illicit adding, deduction, or change of them.

Recovery Time Objective (RTO) : Maximum time allowed to restart the service or operation after a disconnection of the IT services.

Recovery Point Objective (RPO) : the maximum permissible age for data that may be lost when service is restored after an interruption.

Cyber Risk Management : Operations of identifying, measuring, controlling and monitoring cyber risks.

Critical Operations : Operations that cannot be halted for long time, as stated in the company's business impact analysis studies, as well as systemically significant and high-risk company operations.

E-mail : A service that enables users to create, send, receive, and store e-mails using electronic communication systems.

Encryption : The process of transforming information into an unreadable or non-understandable form.

Third Party : The entity to which the company is entrusted to take over its technical and technological tasks, partially or wholly, in order to assist it in carrying out its licensed activities in consistent with the provisions of effective legislations.

Outsourcing : Assign a third party or use its resources to conduct the company's business, or part of its tasks which falls within its responsibility.

Physical Security : Protection standards and procedures that monitor or limit accessing to any of the company's facilities, resources, or information that are stored on physical media, or to prevent access to information resources and systems, such as buildings, files cabinets, personal computers and laptops, servers and equipment.

Stakeholders : Any related party of the company including shareholders, employees, creditors, customers, external suppliers, or relevant regulatory authorities.

Event Log : Data files of security and operational events produced by the system components to understand the system activity and diagnose problems that may occur on it.

Audit Trail : Data files that provide documentary evidence of the sequence of the functional and administrative processes that take place on the systems.

Risk Assessment : Measure and determine the probability of risk occurrence and severity and anticipate its impact on the company.

Penetration Testing : A test wherein specialized assessors attempt to search for security vulnerabilities and circumvent the security features of information systems and security controls and exploit them to try to penetrate those systems from outside or inside the company to test the effectiveness of the security controls used by the company to protect its systems.

Remote Access : Enabling communication with the company's systems from outside its internal network, whether this is for the purposes of its employees remote working or securing the communication with business partners or by third parties.

b-The definitions mentioned in the Central Bank Law, the Electronic Transactions Law, the Banking Law, and any relevant instructions issued by the Central Bank shall be adopted wherever they are stipulated in these instructions unless the context indicates otherwise.

Chapter Two

First: Cyber Security Governance

Article (6):

The Company shall comply with the following:

a. The Board of Directors and its delegated committees, as well as the executive management shall encompass competent persons with appropriate skills and knowledge to understand and manage cyber risks.

b. The Board or its delegated committees according to their positions shall undertake the following responsibilities and tasks:

1. Adopting the Cyber Security Policy.

2. Adopting the Cyber Security Program.

3. Check the compliance with the Cyber Security Policy and Program.

c. The executive management shall tackle the following responsibilities and tasks according to their positions:

1. Ensure that the cyber security policy is implemented and updated.

2. Ensuring the implementation of the cybersecurity program so that it is integrated with the general framework for managing information technology risks, and continuing to update and develop it

3. Ensure that there is a comprehensive Cyber Risk Register and ensure that it is continuously updated and compatible with the company's IT Risk Profile.

4. Monitor and supervise the level of cyber risks continuously.

5. Adopting lists of authorities related to cyber risk and security management in terms of identifying the Responsible, Accountable, Consulted, and Informed parties, entity/entities or person for all process of managing, controlling, monitoring and auditing these risks.

Second: Cyber Security Program and Policy

Article (7):

The Company shall apply and continuously update the Cyber Security Program to ensure that the requirements of confidentiality, reliability and availability of information in the ICT environment are met. The program shall at least include the following:

a. Identify internal and external threats to cyber risk.
b. Identify and classify information risks and sensitivity in the ICT environment.
c. Determine the entities authorized to access and use the information and the ICT environment.

d. Implement cybersecurity policy and procedures and operate the ICT environment that is required to ensure the protection of information assets and sensitive information in the company against illegal penetration.
e. Detect successful and failed illicit penetration attempts upon occurrence if possible.
f. Undertake the necessary corrective procedures to control and mitigate the adverse effects of cyber risks.
g. procedures for restarting the company's operations after its suspension, including those related to the services and legal and regulatory requirements within the accepted time period that specified in the Business Continuity Plan and in accordance with Article (32/ f) of these Instructions.

Article (8):

The cyber security policy shall be a dedicated document to the cyber security in the company. All stakeholders shall participate in setting and updating the policy and adopt the best international practices and their updates including the references, lessons learned from cyber security events. The company can embed the cyber security policy with its information security policy under the name "Information security and cyber security policy", and can embed the cyber security programs with its information security program providing that all the provisions of these instructions be fulfilled.

Article (9):

The cyber security policy shall at least include the following topics:

a. Define the roles and responsibilities, including decision making responsibility within the company with regard to cyber risk management, considering emergencies and crises cases.
b. Data governance and classification.
c. Information security and management and the company's ICT environment.
d. Privacy of customers' data.
e. Cyber risk management.
f. Controls to mitigate and contain cyber risks.
g. Business continuity and disasters recovery plans.
h. Cooperate with stakeholders to respond effectively and recover from cyber attacks.
i. Monitoring and developing systems, networks and applications.
j. Physical and environmental security controls.
k. Managing outsourced operations to third party.

l. Conduct training and awareness programs for the company’s employees regarding cyber security to ensure that all employees implement all the provisions of its cyber security policy.
m. Determine the disclosure mechanism to stakeholders concerning the provisions of the cyber security policy based on their roles.
n. Identify the policy owner, scope of application, periodicity of reviewing and updating, accessibility authorizations, distribution, objectives, responsibilities and related working procedures, as well as penalties for non-compliance and compliance check mechanism.

Article (10):

The company shall manage the security of information related to the cyber security through an information security manager who does not administratively follow the IT department, and shall be independent in a manner that ensures the non-conflicts of interests, and has the practical experience and the professional knowledge required to tackle at least the following tasks:

a. Directly supervise the development of the cyber security program and policy and ensuring their implementation as well as working on reviewing and updating them continuously.
b. Assess the adequacy and efficiency of the cyber security program and policy.
c. Review the effectiveness of the adopted security controls in the company's cyber security policy in a continues manner.
d. Identify and assess cyber risks.
e. Submit reports at least semi-annually, or whenever necessary, to the Board and the Executive management regarding the cyber security in the company. The report shall include at least the following issues:
   1. Misalignments related to the implementation of the cyber security policy and procedures.
   2. Results of cyber risk assessment.
   3. Results of the assessment of the adequacy and efficiency of the cyber security program and policy.
   4. Recommendations, procedures and requirements that must be implemented.
   5. A brief of the most significant cyber threats and attacks events experienced by the company during the reporting period.

Article (11):

Notwithstanding the provisions of Article (10) above, the company shall be entitled to fully or partially outsource the functions of the information security management to a third party, providing compliance with the following:

a. Request the third party to comply with the requirements of these instructions regarding information security management.
b. Check the compliance of the third party with the requirements of the instructions regarding information security management.

Article (12):

The company shall and before making any change in the information and communication technology environment in the company, operations or procedures, or after the occurrence of any event affecting the company's security, ascertain whether there is a need for changes or improvements to the cybersecurity policy and program.

Chapter Three

Cyber Risks Management

First: Identifying Critical Operations and Information Assets in the Company

Article (13):

The Company shall determine the following in order to be able to assess the cyber risks that it may encounter:

a. Critical functions and operations in the company.
b. The company’s information assets, and understand its operations, procedures, systems and its related resources and information systems and their access methods including its internal and external systems.

Article (14):

The company shall classify its functions, critical operations and information assets according to their importance and sensitivity, and continuously review and update these classifications.

Second: Cyber Risks Assessment

Article (15):

The Company shall conduct ongoing Cyber Risk Factor Analysis in terms of determining the following issues:

a. Internal threats.
b. External threats.
c. Vulnerabilities of the ICT environment resources management.
d. Vulnerabilities of the ICT environment's capacity to enable the company's operations.
e. Vulnerabilities of the ICT environment risk management.

Article (16):

The company shall perform the Cyber Risk Scenario Analysis continuously in terms of determining at least the following issues:

a. Source of cyber threat: whether internal or external.
b. Type of cyber threat: either natural, artificial, or technological.
c. Cyber event: for example, but not limited to, the disclosure of confidential information, illicit disruption or modification, steal, destruct, ineffective design, or unacceptable use.
d. Assets or resources affected for example, but not limited to, human resources, organizational structures, ICT environment, operations, or information.
e. Time: the time of occurrence, the duration of the event, and the age of the event when detected.

Article (17):

The Company shall set out a Cyber Risk Register and update it continuously; the register shall include at least the following:

a. Asset’s owner, assessment team, assessment date, subsequent assessment date, summary of cyber risk assessment and management options.
b. Cyber risks assessment, in terms of measuring the two dimensions of risks presented by the likelihood of the event (potential) and its impact or severity. It is preferred to use an even standard scale for the assessment dimensions and to illustrate the magnitude of the impact according to the company’s objectives and operations that includes information technology using the assessment parameters of one of the following international models, for example:
    1. COBIT Information Criteria.
    2. Balanced Scorecard (BSC).
    3. Extended BSC.
    4. Wester man.
    5. COSO ERM.
    6. Factor Analysis of Information Risk (FAIR).
c. Risk Appetite.
d. Options of Risk management (acceptance, mitigation, avoidance, transference).
e. Risk management plan clauses and following up their implementation (implemented or under implementation as planned).
f. Key Risk Indicators, to ensure that acceptable risks and risk tolerance levels are not violated (The percentage of deviation that have been added to the acceptable risk).
g. Standards to assess the confidentiality, integrity, security, and availability of the systems and sensitive information.
h. Defining the responsibilities of the company's employees towards those risks.

Article (18):

The Company has the right to assign a third party to assess cyber risks, considering the compliance with the provisions of effective legislations.

Chapter Four

Protection Controls

First: Protection of Systems, Software, Networks and Network Devices

Article (19):

The Company shall put in place the following protection controls, for example, but not limited to, for all components of the ICT environment, such as systems, software, networks, and network devices against any cyber event:

a. Isolate networks to ensure that the impact of systems vulnerable to a cyber attack is separated from others upon its occurrence, in a manner that facilitates retrieving services efficiently and effectively according to the company's cyber risks assessment.
b. Separate the infrastructure’s sites (main and disaster recovery site) of critical systems in a secure and limited access area, as well as documenting visitors’ entry records to this area, and put in place monitoring systems for infrastructure’s sites.
c. Isolate the test and development environment of critical systems from the production environment.
d. Assess the degree of efficiency of the networking design and the network devices including security devices (such as Firewalls, Intrusion Prevention Systems (IPS)) continuously to meet business needs and maintain an updated networking design in the company. Also, keep an up-to-date list of devices connected to the company's network and schematic diagram of the data center in the main and disaster recovery site in a safe place, which be accessed only by authorized persons.
e. Provide proactive measures to prevent connecting other parties or employees’ devices with the networks, servers and systems of the company, including personal computers, laptops, and any other devices without obtaining the necessary approvals and implement the policies and guidelines of information security and cyber security on them in case the approval of connecting, as well as providing a set of controls to detect whether any devices are illicitly connected to the company’s networks and systems.
f. Provide the necessary hardware and software to monitor, warn, and detect penetration and illegal access such as Intrusion Detection Systems and antivirus programs and ensure that they are continuously updated and used effectively in the monitoring and intrusion detection operations.

g. Update the operating systems and software installed on the devices and servers of the company's critical systems with the latest updates recommended by the provider especially updates related to addressing the security vulnerabilities by the providers of these systems to avoid the risks of non-updated systems, in line with the company's Patch Management Policy. Providing that change management policies and procedures are implemented as quickly as possible and make decisions based on information technology risks and cyber risks and provide effective alternative controls when this can't be applied. In addition, the company shall delete any software or files stored on critical systems servers which are not relevant to the company's programs taking into consideration conducting the required tests prior implementing these updates on the systems.

h. Restrict employees' access to the internet to trusted sites only.

i. Separating the processes of employees' access to critical systems from their access to the internet. If otherwise required, the necessary approval must be obtained and documented.

j. Establish standards for the security settings of the ICT environment according to the best practices, and documenting that.

k. Establish procedures and guidelines designed to ensure the safety of programs and applications development processes within the company's environment, in addition to the procedures of evaluating or testing the security of the programs and applications developed outside the company's environment.

l. Reviewing and developing all the procedures and guidelines designed to ensure the safety of programs and applications development practices, periodically, by qualified people, and according to the international standards in this regard.

m. The company shall determine the activities that may endanger its systems, specially the financial systems and circulate them among the employees to prevent being engaged in it.

n. Employ encryption systems that are highly reliable for sensitive files stored in devices or transferred over networks.

Article (20):

The company should employ protection systems of various sources within different levels (Different Security Tiers), on all its critical systems.

Article (21):

The company should provide the following protection controls for critical systems and sensitive data in the company regarding the authentication /verification of the users identity of these systems:

a. Employing strong and effective access controls (Strong Authentication) through two or more authentication factors (Multi-factor Authentication) according to the level of risks, while ensuring appropriate separation between them in a way that minimizes the possibility of others to know one factor through the other one, in addition to use the necessary means and techniques that guarantee the accountability and non-repudiation.

b. In the event of an urgent need for remote access, it should be used with minimal limits, with the necessity to provide access controls through multiple authentication / verification means and use of highly reliable encryption techniques and other accompanying controls to reduce the risk of unauthorized penetration.

c. Applying international security standards and best global practices when choosing password specification.

Article (22):

The company should provide the following protection controls concerning the information related to its activities:

a. Disposal of any sensitive information that is no longer necessary for running the critical operations in the company, in compliance with the laws, bylaws, and instructions issued in this regard.

b. Ensuring the availability of information related to the company’s work through periodically taking backup copies in safe locations inside and outside the company’s premises.

c. Committing to the data classification policy when sending messages with confidential content and encrypting those messages according to their sensitivity.

d. Activating the necessary controls to protect the confidentiality of sensitive information retained or transferred through external networks, including the encryption of that information.

e. If the company is unable to encrypt the sensitive information that is stored and used in messaging, it should protect the sensitive information by alternative and effective methods to be reviewed and authenticated by the information security manager.

Article (23):

The company should provide the following protection controls regarding the access controls to its systems:

a. Continuous monitoring of user activities whom authorized to use and access the company's systems and networks and detecting access to identify unauthorized usage or modification of sensitive information.

b. Employing the necessary protection controls to control access to the company's systems, servers, and software, and continuously review the granted authorities for the usage and access to these systems, and ensuring their appropriateness to the nature of work and their legitimate usage also instantly eliminating unused authorities and identification codes, through providing an authority matrix for the systems approved by the senior executive management, clarifying the authorities given depending on the position level for all systems so that the authority matrix should consider the following principles:

   1. Segregation of duties.
   2. Dual control on sensitive operations.
   3. Granting authorities according to the need.

c. Reviewing and amending the authorities on a periodic basis and upon occurrence of any change on the systems or job titles.

d. Compliance and monitor the compliance to the password policy, with concentrating on the necessity of changing the default passwords accompanying new systems and devices immediately upon usage.

e. Applying the rule of granting least privileges and on a need to know need to do, provided that these privileges are reviewed continuously.

f. Adopting the access rule which states that access is generally prohibited except for what is permitted.

g. Avoid using shared/ generic accounts.

Article (24):

The company should provide the following protection controls regarding the risks of internal cyber threat:

a. Monitoring and analyzing the activities of people unauthorized to access the company's ICT environment in case of their unauthorized access attempt to the ICT environment.

b. Employing data loss detection techniques, and protection techniques against changing or leakage of classified data from the company's network.
c. Setting appropriate recruitment rules for new employees, especially for those whose work is associated with the critical systems, to verify their employment record if exists.
d. Conducting a comprehensive check for new employees, as well as, conducting similar check processes for all staff at regular intervals throughout their entire employment period, commensurate with staff's access authorities and their usage of critical systems.
e. Activating the necessary controls to manage the risks associated with the employees who terminate their work at the company or temporary stop working for long periods especially due to suspicious behavior.
f. Contracts signed with the employees should include clear legal provisions in case they breach the systems or access the systems in an unauthorized manner, or signing a pledge form in this regard, in accordance with the relevant legislations in force and the company's systems.

Second: E-Mail Protection Controls

Article (25):

a. The company should apply a policy for managing and defining applications, protocols, and the e-mail domain bearing the company's name over the internet, including the implementation of the following secure controls and standards for the e-mail system as a minimum:
   1. Allowing the e-mail user to access his own account only after verifying his identity, and by following an authentication/verification method that is difficult for others to penetrate. A multi-factor authentication method can be used, especially for users whom their work is considered sensitive and carry out implications and risks on the company's operations and its reputation.
   2. Employing highly reliable encryption techniques for the classified information to ensure the protection of the processes of connecting to the e-mail.
   3. Activate the "Reverse DNS Check" feature to verify that the digital address (IP) of the sender of the (incoming) email matches the domain and device names that issue that email.
   4. Disable the feature of receiving mail from sources which allow the open mail relay.

5. Activating the real-time blocking list (RBL Check) feature, by which messages incoming from suspicious sources are blocked depending on reliable and updated international data lists in this regard, in addition to internal data lists built and updated for achieving the same purpose.
6. Activating the sender policy framework (SPF Check) feature whenever possible in a way that contributes to reducing of the possibility of receiving e-mail messages from non-original sources.
7. Considering the possibility of activating the "DNSSEC" feature within the components of the technical environment of the company.
8. Blocking the suspicious attachments and links within e-mail messages, through testing them by software dependable in this regard, restricting the executable files, and identifying a permitted maximum attachment size limit, with the necessity of activating an appropriate policy for the e-mail system to deal with those messages according to the degree of their risks.
9. Consider the possibility of defining limits for the number of connections to the e-mail server from a single source in accordance with the e-mail server specifications and work requirements wherever needed.
10. Employing availability features and business continuity plans for e-mail services according to the business impact analysis (BIA).
11. Maintain tracking records for the e-mail systems owned by the company for a period set within the data retention policy, of not less than three months.

b. Setting a policy concerning the usage of e-mail based on best international practices in this field, with adherence to the data classification policy when sending messages with confidential content and encrypting those messages.

c. Working on developing an awareness program, which should be continuously updated and directed to e-mail users regarding the mechanism of dealing with and detecting fraud and suspicious e-mail messages, which specifically includes the possibility of communicating with the e-mail sender in case of doubting the identity of the sender through other means of communication.

Third: Records

Article (26):

The company should commit to the following:

a. Providing event logs and audit trails for the ICT environment and the systems operating on it.
b. The existence of a mechanism for administrating, analyzing and monitoring event logs and audit trails continuously according to the classification of the importance of the systems operating on the ICT environment and documenting that.
c. Determine the types of records which have to be retained and their retention periods and the authorizations to view them.
d. Providing the necessary protection for event logs and audit trails to ensure its availability and integrity.
e. Providing an appropriate mechanism to verify that the event records are reviewed for the ICT environment by an independent party inside or outside the company in a manner that does not contradict the provisions of the legislation in force.

Chapter Five

Detecting Cyber Events

Article (27):

The company should detect the vulnerabilities in any of the components of the ICT environment in the company. The detection capabilities should also address misusage of those systems by others, internal possible threats and other advanced persistent threats.

Article (28):

The company should put in place multi layers controls for the detection process to cover people, operations and technology, while using each layer as a safety net for the previous layer. The company should also undertake an approach, which enables it to delay, disable or stop the ability of proceeding in the stages of a cyber attack sequence.

Article (29):

The company's detection capabilities should be able to support the process of response to events and collect the information and evidences necessary for the forensic IT audit process whenever needed.

Article (30):

The company should provide the necessary mechanisms and systems to perform continuous monitoring and find correlations to detect the unusual activities and events which may affect the activities of the company or cause a financial loss.

Article (31):

Measures must be implemented to detect potential leaks of information, malicious code, security threats, vulnerabilities and security holes, and the need to follow up on the latest security updates, verify and apply these updates on an up-to-date basis.

Chapter Six

Emergency Cyber Events Response and Recovery

Article (32):

The company should provide the following response controls for emergency cyber events:

a. Establish a plan for responding to cyber events, which designed for immediate response and recovery from any emergency event, related to the cyber security of the company.
b. The response plan for cyber events should include at least the following:
    1. Determine the roles and responsibilities for taking decisions in a clear manner.
    2. Internal processes concerning the response to cyber events.
    3. Objectives of the cyber events response plan.
    4. Internal and external communications and information exchange with stakeholders.
    5. Determine the requirements necessary for treating any vulnerabilities in any of the ICT environment components and the related controls.

6. Cyber events risks.
7. Documentation and reporting regarding cyber security events and the relevant event response activities.
8. Evaluate and review cyber events response plan as needed posterior to the cyber event.
9. The locations of storing the plan (Hard copy, Soft copy) and the related procedures.

c. Testing the cyber events response plan, and continuously updating it, based on the current information on cyber threats and lessons learned from previous events which the company or any other company, inside or outside the kingdom, was exposed to.

d. Cooperating and coordinating with stakeholders to assist in responding to cyber events, with the aim to contain these issues and unexpected events, and minimize their effects, especially if their systems are connected to the company's systems. Also cooperate with them when setting the cyber events response plan.

e. Conducting a comprehensive investigation and evaluation when detecting a successful cyber attack or an attempt for a cyber attack, to identify its nature, scope and subsequent damages. The company should also undertake immediate procedures to contain the cyber event to prevent more damages and to restore its operations based on the cyber events response plan.

f. Designing and testing all of its systems and operations, so that the recovery time objective for its Critical Operations (RTO) is consistent with the instructions and circulars issued by Central Bank of Jordan in this regard. Response scenarios should also be set in case of a failure to resume during that period.

g. Designing and testing its systems and operations to enable the restoration of sensitive data after the occurrence of cyber attack. In addition, strict controls should be set to detect and protect this data.

h. An agreement with stakeholders should be established regarding the recovery point objective (RPO), and the recovery time objective (RTO) for each information technology service, documenting it and using it as requirements for designing the service and information technology continuity plans.

i. Procedures that enable it to identify the party responsible for addressing the vulnerabilities which appeared as a result of the investigation in an emergency cyber event to prevent further damages, contain the event, repair the damages, and prevent recurrence of the event in the future.

Article (33):

The company should set procedures for the recovery from cyber events. These procedures should include the following:

a. Eliminating the effects of harmful events.
b. Ensuring that the systems and data return to their normal state.
c. Identifying, mitigating and addressing the vulnerabilities that have been exploited to prevent similar events from occurring.
d. Appropriately communicating with all internal and external stakeholders regarding the recovery from the cyber event.

Chapter Seven

Testing

Article (34):

The company should test the components of the ICT environment after the occurrence of the cyber event in coordination with stakeholders.

Article (35):

The company should commit to the following:

a. Implementing penetration tests for critical systems at least once a year or after implementing a radical adjustment to the company's system/systems, taking into consideration the following:
   1. Building the testing scope based on the sensitivity of the systems and its related supported systems.
   2. Implementing the tests on the level of applications as well as internal and external networks in the company.
   3. The possibility of implementing the tests by a third party, provided that they are not outsourced to the same third party for more than two consequent years.
b. Implementing an assessment for vulnerabilities and security gaps of critical systems and its supported systems as well as internal and external networks, periodically, according to the Central Bank of Jordan instructions and circulars that have been issued in this regard, and undertaking the procedures to address the detected gaps.

c. Monitoring the company's systems continuously and effectively to detect any defect in any of the components of the ICT environment which may indicate the existence of new gaps.

Article (36):

The company should set a comprehensive evaluation program to verify the effectiveness of the cyber security policy and program on a regular and a frequent basis, provided that the board and executive management are appropriately informed with the results of that evaluation.

Chapter Eight

Outsourcing

Article (37):

The company should evaluate the need for outsourcing critical operations to a third party depending on a comprehensive evaluation for cyber risks, taking into consideration the provisions of the related legislations in force.

Article (38):

The company should commit to the following, in case part of the company's operations is outsourced to a third party:

a. The company should ensure that the necessary protection controls are in place to control all cyber risks related to its sensitive data and systems, its clients that are being hosted by the third party. Also, perform periodic and regular tests to evaluate those controls by independent parties and obtain reliable assurances in accordance with the internationally accepted standards in this regard and these instructions and/or continuous supervision and oversight of the services provided by the third party.

b. The board and senior executive management of the company should establish a system and a mechanism for managing the services provided by the third party with the aim of supporting the process of providing the company's services and embedding this in the company's outsourcing policy.

c. The company should sign a non-disclosure agreement with the third party.

d. The effective legislations and specifically those related to banking privacy and the privacy of clients' data and its protection.
e. Any conditions or requirements identified by the Central Bank of Jordan in this regard.

Article (39):

The company should include the following items within its outsourcing policy regarding cyber risks taking into consideration the provisions of the legislations in force:

a. Procedures to control the third party's remote access including the necessity of access through multi-factor authentication to limit its access to the related systems and sensitive information.
b. The controls that should be used by the third party related to the encryption for protecting the company's sensitive information while it is being transmitted or stored by that party.
c. The notification that the third party should provide to the company in case of the occurrence of a cyber-security event that directly or indirectly affects the company's systems or its sensitive information that held by the third party.

Article (40):

Singed contracts between the company and the third party should include the requirements of these instructions, especially the following:

a. When signing outsourcing agreements with the third party, the company should ensure the third party's commitment to implement the provisions of these instructions to the extent that is appropriate to the company's operations importance and nature, as well as the services, programs and infrastructure provided to the company before and during the contract period. While not exempting, the board and the executive management from the ultimate responsibility to achieve the requirements of these instructions, provided that to reconcile the status of the companies that are currently contracted with the company at the instructions date entry into force or during the contract period whichever is earlier.
b. The audit right of the company to evaluate the cyber risks emerging from the third party's practices that effect the company, by another neutral and reliable party including providing assuring letters about its opinion regarding testing the controls and their adequacy, according to the international standards followed in this respect.
c. The minimum level of cyber security practices required to be fulfilled by the third party including the necessary security procedures regarding the service level.
d. The third party's commitment to the cyber security policy of the company.

e. The third party should provide the company with instant reports regarding any cyber attacks attempt or emergency events that the company's data and services may be exposed to at the third party.

Chapter Nine

First: Training and Raising Awareness

Article (41):

The company should regularly raise awareness and train all its employees among all their levels to enhance the literacy of the importance of cyber security inside the company, though it should be updated to reflect the risks identified by the company in its risks assessment including at least the following:

a. Awareness regarding cyber security and types of cyber threats.
b. How to detect cyber risks and address it.
c. How to report about any non-regular activity or event.
d. Emergency plans and methods of responding to emergency cases and the embezzlement, forgery and cyber attack cases.
e. The mechanism for implementing the instructions and raising awareness of the tasks, responsibilities and consequences of accountability in cases of non-compliance.
f. Best international practices regarding how to use the systems and networks for controlling and managing cyber attacks risks, providing employees and inform them about the company's information security policies, cyber security policy and signing them with an endorsement regarding understanding and commitment to the content of these policies.

Article (42):

The company should provide special and intensive training for the employees who work in the information security and cyber security field, as well as the employees who have authorities to access critical systems and sensitive information according to their positions.

Article (43):

The company should provide awareness programs to board members and executive management on the information technology and cyber security risks and best international practices in this regard at least once a year.

Article (44):

a. The company should aware its clients to avoid the risks of cyber attacks and the need to follow controls to preserve their financial and banking data and to take caution and prudence, such as:
    1. Learning and understanding the security and privacy policy for the company's websites and applications.
    2. Protecting the personal identity and identification data through using different recognition indicators for different web applications, and minimize the sharing of personal information on websites or applications that require this information.
    3. Notifying stakeholders about the suspicions events they are facing.
    4. Not sharing the banking information on untrusted websites or applications that require this information.
    5. The necessity of continuously increasing the clients' awareness about how to verify the company's identity on the internet and through phone applications when using its services.

b. The company should clarify the reliable and secure methods to report on any cyber-attack or data theft for the stakeholders.

Second: Exchange of Cyber Events Information

Article (45):

The company should exchange cyber events information at the appropriate time with the stakeholders as well as with reliable entities specialized in cyber risks that are currently prevailing, as well as the threats, vulnerabilities, events and responses, to enhance the activated controls in the company and limit the damages and increase awareness in line with any circulars or instructions issued by the Central Bank of Jordan in this regard.

Article (46):

The company should depend on internal and external cyber events data in the cyber risks assessment that indicated in chapter three above.

Chapter Ten

General Provisions

Article (47):

The company should discontinue working with the services, systems and devices that are no longer being used and not needed in accordance with the adopted company's policy in this regard and in such manner to ensure that other services, systems or operations are not affected.

Article (48):

The company should adopt and activate a comprehensive change management policy, taking into account the cyber risks before, during and after the change, and implementing a cyber-risk assessment and taking into consideration the controls resulting from the risk assessment process when applying the change.

Article (49):

a. The company should notify the Central Bank of Jordan in case it has detected its exposure to any cyber event or any attempt to a high risk cyber attack to its systems or networks no later than 72 hours from the moment of discovering the cyber event and according to the mechanism adopted by the Central Bank and notify the competent security bodies about any case of embezzlement, forgery, theft or fraud resulting from the cyber event immediately upon discovery and in accordance with the relevant laws and instructions.

b. Providing the Central Bank with the details of cyber events, their effects, response procedures and the implemented preventive procedures, periodically, and according to the mechanism that will be adopted by the central bank.

Article (50):

The company should disclose its cyber security policy with the stakeholders.

Article (51):

The company should inform the client of any updates regarding security procedures that should be followed by him according to the mechanism agreed upon with the client.

Article (52):

internal and external auditor programs must include mechanisms that ensure continuous supervision and follow up for the provisions of the instructions above.

Article (53):

The company should make sure that all the systems and equipment used in the company are compliant with the international and local standards.

Article (54):

The Central Bank of Jordan has the right to demand any reports, data, or records which believes appropriate.

Governor

Dr. Ziad Fariz