Regulation of the National Bank of Georgia on Cybersecurity Management Framework of Commercial Banks

Approved by Decree N. 56/04 of March 22, 2019

of the Governor of the National Bank of Georgia

On the Approval of the Cybersecurity Management Framework of Commercial Bank

According to Article 15 of the Organic Law of Georgia regarding "The National Bank of Georgia",

I hereby state the following:

Article 1.

Approve the Cybersecurity Management Framework of Commercial Banks with the following text.

Article 2.

This Decree shall go into force on April 1, 2019.

Governor of the National Bank of Georgia **Koba Gvenetadze**

Requirements for the Establishment of a Cybersecurity Management Framework by Commercial Banks

Article 1. General Provisions

1. All commercial banks, both resident and branches of non-resident foreign banks operating in Georgia must establish a Framework (hereinafter Framework) for cybersecurity management.
2. The Framework must be appropriate and commensurate with the bank's size and complexity and the nature of its business.
3. The Framework must be fully integrated into the bank's overall risk management process.

Article 2. Cyber-Security Framework

The framework should consist of the following primary functions:

a. Risk Identification - Cyber security risk awareness throughout the organization, which implies and includes cybersecurity risk management. This includes managing cybersecurity risk related to organization's systems, assets, data and processes.
b. Protection – The development and implementation of appropriate controls within the organization in order to ensure the provision of services to the public and other stakeholders.
c. Discovery – The development and implementation of mechanisms for the detection of cyber-security events.
d. Response – The development and establishment of mechanisms for responding to cyber security events.

e. Restoration – The development and establishment of a plan for formal restoration after the occurrence of cyber security events.

Article 3. Identification

Commercial banks must create and implement a cybersecurity risk (cyber-risk) identification process that includes the following components:

a) Asset management, which comprises of:
    a. The full accounting of physical equipment, hardware and information systems of the organization;
    b. The full accounting of the software and potential other information systems being used by the organization.
    c. The Establishment and identification of communication channels and information flows existing within the organization;
    d. The establishment of a catalog of external information systems used by the organization;
    e. A formalized system that includes the classification of existing resources in the bank, according to criticality and business priority.
    f. The establishment of roles and responsibilities of all employees of the organization in a clear and understandable way in terms of cybersecurity risk management.
    g. In relationships with third parties, the determination of the roles and responsibilities in an understandable and clear manner, in relation to the organization's suppliers and clients.
  a. The Business Environment, which includes the following:
    i. Determining the role of the organization in the country's critical infrastructure (if any);
    ii. Determining the role of cybersecurity within the organization's mission, aims and activities;
    iii. Determining attitudes and functions within the delivery of critical services / processes;
    iv. Providing high level of business continuity within the scope of critical service delivery.
  b. Management:
    i. The organization should have an information security policy;
    ii. Within the extent of information security, all the roles and responsibilities should be defined and in compliance with the internal roles of employees in the organization. This also applies to external parties that are connected to the organization;
    iii. The legal and regulatory requirements of the organization in the field of cyber security, In terms of civil liberties and identity protection;
    iv. Executive management and risk management processes of the organization should include cybersecurity risk (cyber-risk).
  c. Cybersecurity Risk Assessment:
    i. The organization's information assets should be formally identified;

ii. The bank should receive information on threats and weaknesses from different forums and sources of exchange of information;
iii. Internal and external threats must be formally identified;
iv. The potential impact of cyber security events on the organization should be identified;
v. The organization should use a specific methodology in order to identify the threats, weaknesses, probabilities, and impact to determine the cybersecurity risk;
vi. Bank's risk tolerance and appetite should be in line with the role and importance of the bank in critical infrastructure (if such a role has been established).

Article 4. Protection

1. The process of protection established by the Bank shall consist of the following components:
   a. Access Control:
      i. The Bank shall have a comprehensive management process in place for authorized users and equipment;
      ii. The Bank shall be responsible for managing and protecting access to information assets of its own;
      iii. The organization shall be responsible for managing, ensuring and controlling physical access;
      iv. Remote access to information assets should be fully managed by the bank;
      v. Determining the rights of access by the Bank shall be carried out in compliance with the principle of minimum privilege and the principle of separation of duties/obligations;
      vi. The maintenance of network integrity should be carried out based on the principle on network separation (segmentation), where possible.
   b. Awareness and training:
      i. The bank shall be responsible for cybersecurity training at least once in a year for all of the employees of the organization, including executive, middle management and operational employees;
      ii. All users should be informed and trained on cyber-risk;
      iii. The Bank's privileged users should be aware of their own role and obligations taken before the organization;
      iv. Third Parties of the Bank should be aware of their respective cybersecurity roles and responsibilities;
      v. Within the context of Cybersecurity, the Executive Management of the Bank should be aware of its own role and responsibilities;
      vi. The Bank's physical and information security staff should be well-aware of their roles and responsibilities.
   c. Data protection:
      i. Static data (data-at-rest) of the Bank must be properly protected;
      ii. Data-in-transit existing in the bank must be adequately protected;
      iii. The bank must fully manage all information assets (including removal, transfer, storage and disposal);
      iv. The Bank shall have adequate mechanisms for the prevention of data leakage;

v. The Bank should have a mechanism for checking the software, data / information integrity;
vi. Software development and testing environments should be separated from each other.

d. Information security processes and procedures:
   i. Baseline configuration of information technology should be created and maintained by the Bank;
   ii. Systems development lifecycle should be implemented;
   iii. The organization should have a formal mechanism / process for managing the configuration of systems;
   iv. The organization must have formal mechanisms for data / information backup / storage, which includes testing of the information restoration process;
   v. Data in the bank should be destroyed according to the Bank's relevant policies;
   vi. The process of protecting the information assets of the bank must be constantly improved;
   vii. The efficiency of defensive technologies should be analyzed regularly;
   viii. The Bank shall have an incident response plan;
   ix. The Bank shall conduct regular testing of the Incident Response Plan;
   x. The bank should develop and implement a vulnerability management plan.

e. Maintenance:
   i. The Bank shall be responsible for the timely maintenance and repair of organizational assets, which are performed and logged with approved and controlled tools;
   ii. Remote management / maintenance of the bank's information assets shall be formally approved, recorded and executed so that unauthorized access is restricted;

f. Protective technologies
   i. The Bank shall have a formal mechanism for accounting and keeping an audit trail, which corresponds to the Bank's policy;
   ii. Portable equipment must be protected and their use in the bank should be limited to the Bank's policy;
   iii. Access to organization's systems and assets must be formally controlled, incorporating the principle of least privilege access;
   iv. The bank's communication and management network should be protected.

Article 5. Discovery

1. The process of discovery by the bank related to cyber security events should consist of the following issues / components:
   a. Anomalies and events
      i. The Bank should establish a baseline of network operations and expected data flows/streams for information systems and consumers;
      ii. The organization should analyze discovered events in order to study potential cyber-attack targets and methods;
      iii. Summarize the events related to cybersecurity events and potential correlation with different sources;

iv. The Bank shall have an incident warning mechanism, with appropriate risk indicators and other metrics:

b. Detection processes
   i. The Bank should have clear roles and responsibilities related to the discovery of cybersecurity events;
   ii. Testing of event detection processes (relevant controls) should be performed;
   iii. Information relating to the discovery of specific events should be communicated to the relevant persons and agencies;
   iv. The constant improvement of the process of discovering the events of the organization shall be performed.

Article 6. Response

1. The response to cybersecurity events should be based on the following issues / components:
   a. Response Planning
      i. Banks should have a formal response plan related to cybersecurity events;
      ii. The response plan must be put into effect when reporting a particular event, or after the event is recorded;
   b. Communication
      i. Bank staff should be well aware of their role in responding to cyber security events;
      ii. Notification of cyber security events should be carried out in accordance with established requirements and criteria;
      iii. Information related to cyber security events should be done in accordance with the Response Plan;
      iv. Coordination of activities related to cybercrime events should be coordinated with other agencies in accordance with the Response Plan;
   c. Analysis
      i. The Bank shall carry out an analysis of information received from detection systems;
      ii. The organization should fully understand the impact of the cyber-security incident on the organization;
      iii. In case of need, an expert examination should be carried out;
      iv. The Bank must classify incidents in accordance with the Incident Response Plan.
   d. Mitigation
      i. The Bank's obligation is to mitigate the impact of cyber-security incidents if an incident has occurred in the bank;
      ii. The Bank shall be responsible for studying recently discovered weaknesses and mitigating / receiving threats due to these weaknesses, if the weakness is not a significant threat to the organization;
   e. Improvement
      i. Bank's Incident Response Plan should include past experience and practice;
      ii. Regular updating of the incident response strategy should be done.

Article 7. Restoration

1. The process of recovery from the cyber-threat event should consist of the following components:
    a. The Bank must have a formal mechanism for restoration of operations after a cybersecurity event has occurred;
    b. The restoration process should, in turn, take into account the experiences from past events;
    c. The Bank should have a formal procedure and mechanism for public relations within the framework of which the bank provides information to the public about a cyber security incident, and if necessary, for reputation risk management.
    d. The Bank shall be responsible for notification of the actions related to specific events with internal stakeholders, including the management of the organization.

Article 8. Cyber Security Program Management

1. Management of the Bank is obliged to regularly check the efficiency of the organization's cyber security / information security program.
2. The organization shall conduct annual self-assessment of cyber security.
3. The Bank shall conduct a penetration test at least once a year, which includes all the information systems of the Bank that are connected to the network.
4. The Commercial Bank shall conduct an annual independent audit of all components of the Bank's Cyber Security Management Framework. The information security audit must include risks associated with confidentiality, integrity and availability of systems.