On approval of the Rules for assessment of level of protection against information security threats

Unofficial translation

Resolution of the Board of the Agency of the Republic of Kazakhstan on regulation and development of the financial market dated November 23, 2020 No. 110. Registered in the Ministry of Justice of the Republic of Kazakhstan on November 27, 2020 No. 21685

Unofficial translation

This resolution comes into force on January 1, 2021.

In accordance with subparagraph 1) of part 1 of Article 13-6 of the Law of the Republic of Kazakhstan dated July 4, 2003 "On state regulation, control and supervision of the financial market and financial organizations", the Board of the Agency of the Republic of Kazakhstan for regulation and development of the financial market DECIDES:

1. To approve the attached Rules for assessment of the level of protection against information security threats. 2. The Cybersecurity Department, in the order established by the legislation of the Republic of Kazakhstan, to ensure:

1) jointly with the Legal Department, a state registration of this resolution in the Ministry of Justice of the Republic of Kazakhstan;

2) posting of this resolution on the official Internet resource of the Agency of the Republic of Kazakhstan for regulation and development of the financial market after its official publication;

3) within ten working days after the state registration of this resolution, submission of information to the Legal Department on implementation of the measure provided for in subparagraph 2) of this paragraph.

3. The supervising Deputy Chairman of the Agency of the Republic of Kazakhstan for regulation and development of the financial market is authorized to control the execution of this resolution.

4. This resolution comes into force on January 1, 2021 and is subject to official publication.

Chairperson of the Agency of the Republic of Kazakhstan for regulation and development of financial market — *M. Abylkasymova*

Approved
by the resolution of the
Board of the Agency of the
Republic of Kazakhstan for
regulation and development of
financial market
dated November 23, 2020 № 110

Rules for assessment of level of protection against information security threats

Chapter 1. General provisions

1. These Rules for assessment of the level of protection against information security threats (hereinafter referred to as the Rules) are developed in accordance with the Law of the Republic of Kazakhstan dated July 4, 2003 "On state regulation, control and supervision of the financial market and financial organizations" and determine the procedure for assessment of the level of protection against information security threats of financial organizations and branches of non-resident banks of the Republic of Kazakhstan, branches of insurance (reinsurance) organizations-non-residents of the Republic of Kazakhstan, branches of insurance brokers-non-residents of the Republic of Kazakhstan (hereinafter - financial organizations).

2. The following concepts are used in the Rules:

1) key information systems of a financial organization - information systems of a financial organization necessary for functioning of business processes that implement the main activities of a financial organization;

2) an authorized body - a state body exercising state regulation, control and supervision of the financial market and financial organizations.

Chapter 2. Procedure for assessment of level of protection against threats

3. Assessment of the level of protection against information security threats is carried out by financial organizations at the request of the authorized body.

4. The assessment of the level of protection against information security threats is carried out by the financial organization in accordance with the parameters for assessment of the level of protection against information security threats in accordance with the appendix to the Rules.

For each parameter specified in column 2 of the appendix to the Rules, the financial organization determines one of the levels of security specified in columns 3, 4, 5 of the appendix to the Rules.

5. The assessment of the level of protection against information security threats is drawn up by the financial organization in the form of a table indicating the parameters for assessment of the level of protection against information security threats listed in column 2 of the appendix to the Rules, the level of protection and a brief description of their implementation.

6. The result of assessment of the level of protection against information security threats is approved by the head of the financial organization and provided by the financial organization with a cover letter to the authorized body within a period not exceeding three

months from the date of receipt of the request from the authorized body for such an assessment.

7. The results of assessment of the level of protection against information security threats by the financial organization are accompanied by documents confirming the levels of protection 2 and 3 in accordance with the appendix to the Rules.

8. The authorized body checks the results of assessment of the level of protection against information security threats provided by the financial organization for compliance with the attached documents and determines the final level of protection of the financial organization for each of the parameters for assessment of the level of protection against information security threats in accordance with the appendix to the Rules.

9. The final results of assessment of the level of protection of a financial organization against information security threats are brought to the attention of the financial organization by the authorized body.

Appendix
to the Rules for assessment
of level of protection against
information security threats

Parameters of assessment of the level of protection against information security threats

№	Parameter of assessment of the level of protection against information security threats	Level of protection 1	Level of protection 2	Level of protection 3
1	2	3	4	5
1.	Financial organization approved and notified all employees of the financial organization, as well as third-party organizations, of a document containing a description of the information security policy.	There is no document describing the information security policy.	An approved document containing a description of the information security policy is available.	An approved document containing a description of the information security policy is available and communicated to all employees and third parties.
2.	Financial organization analyzes and revises the document containing the description of the information security policy at specified intervals or when significant changes occur.	The frequency of revision of the document containing the description of the information security policy has not been approved.	The frequency of the revision of the document containing the description of the information security policy has been approved, there is no documentary evidence of the revision within the approved period.	The frequency of revision of the document containing the description of the information security policy has been approved , there is documentary evidence of the revision within the approved period.
	Financial organization approved a document defining the responsibilities of employees and	There is no document that defines the responsibilities of managers and	There is an approved document that defines the responsibilities of	There is an approved document defining the responsibilities of

3.	management of the financial organization to ensure information security.	employees to ensure information security.	employees to ensure information security.	managers and employees to ensure information security.
4.	Financial institution approved a non-disclosure agreement, which is signed by all employees of the financial organization who have access to confidential information.	There is no a non-disclosure agreement.	An approved nondisclosure agreement is available, but not signed by all employees with access to confidential information.	There is an approved non-disclosure agreement signed by all employees who have access to confidential information.
5.	Financial organization approved procedures that determine the list of persons and the procedure for their interaction with the competent authorities (for example, law enforcement agencies, fire services, an authorized body).	There are no procedures that govern the interaction of employees with the competent authorities	-	There are documented and approved procedures that govern the interaction of employees with the competent authorities.
6.	Financial organization supports the interaction of its information security employees with professional groups, associations and their participation in conferences (forums) on information security.	There is no interaction between information security employees of a financial organization with professional groups, associations and participation in conferences (forums) on information security.	There is no an approved document defining the procedure for interaction of information security employees of a financial organization with professional groups, associations and participation in conferences (forums) on information security, information security employees interact on their own initiative.	There is an approved document defining the procedure for interaction of information security employees of a financial organization with professional groups, associations and participation in conferences (forums) on information security, information security employees are members of professional groups, associations and annually take part in conferences (forums) on information security.
7.	Financial organization arranges external audits of the information security processes of key information systems at regular intervals.	An external audit of information security of key information systems has not been conducted over the past three years.	Over the past three years, an external audit of information security has been carried out for more than half of all key information systems.	Over the past three years, an external audit of information security of all key information systems has been carried out.
8.	Financial organization uses the results of an external audit of information security of key information systems to improve information security.	External audit of information security of key information systems is not carried out.	-	Based on the results of the last external audit of information security of key information systems, measures were taken to improve information security.

9.	Financial organization controls the access of third parties to its information processing facilities.	Third party access to information processing facilities of a financial organization is not controlled.	There is an approved document defining information security when providing third parties with access to information processing facilities.	When providing third parties with access to information processing facilities, information security risks are analyzed and measures are developed to reduce the identified risks.
10.	Financial organization has determined information security measures when providing clients with access to the information systems of the financial organization.	Information security measures when providing clients with access to the information systems of a financial institution are not defined.	There is an approved document that defines information security measures when providing clients with access to information systems of a financial institution.	-
11.	Financial organization's agreements with third-party organizations that have access to information or information assets of a financial organization contain information security requirements.	Agreements with third parties that have access to information or information assets of a financial organization do not contain information security requirements.	Separate agreements with third parties with access to information or information assets of a financial organization contain information security requirements.	All current agreements with third-party organizations that have access to information or information assets of a financial organization contain standardized information security requirements defined by an internal document.
12.	Financial organization approved a document containing a list of key information systems of a financial organization with an indication of the owners.	There is no document containing a list of key information systems of a financial organization.	-	There is a document approved or updated during the last year, which includes a list of key information systems of a financial organization with an indication of the owners.
13.	Financial organization has approved and communicated to all employees of the financial organization a document containing the rules for using e-mail.	There is no document containing the rules for using e-mail	-	There is an approved document containing the rules for the use of e-mail, brought to the attention of all employees of the financial organization.
14.	Financial organization approved and communicated to all employees of the financial organization a document containing the rules for using the Internet.	There is no document containing the rules for using the Internet.	-	There is an approved document containing the rules for using the Internet, brought to the attention of all employees of the financial organization.

15.	Financial organization approved and communicated to all employees of the financial organization a document containing a list of protected information.	There is no document containing a list of protected information.	-	There is an approved document containing a list of protected information, brought to the attention of all employees of the financial organization.
16.	Financial organization approved and communicated to all employees of the financial organization a document containing a list of personal data.	There is no document containing a list of personal data.	-	There is an approved document containing a list of personal data brought to the attention of all employees of the financial organization.
17.	Financial organization approved and communicated to all employees of the financial organization a document containing the rules for classifying information with an indication of the list of classes of information, principles for assigning information to a certain class, and determining the responsibility of employees for classifying information.	There is no document containing the rules for classifying information	-	There is an approved document containing the rules for classification of information, brought to the attention of all employees of the financial organization.
18.	Financial organization approved and communicated to all employees of the financial organization a document containing the rules for labeling information carriers.	There is no document containing the rules for labeling information carriers	-	There is an approved document containing the rules for labeling information carriers, brought to the attention of all employees of the financial organization.
19.	Financial organization has approved a document that defines the roles and functions of departments or employees of a financial organization in information security processes.	There is no document that defines the roles and functions of departments or employees of a financial organization in information security processes.	An approved document is available that defines the functions of the information security department or information security officer of a financial organization.	There is an approved document that defines the roles and functions in the information security processes of the information security division and other divisions or employees of the financial organization.
20.	Financial organization in labor contracts with employees provides for the responsibility of employees for non-compliance with information security requirements, including	Employment contracts with employees do not provide for employee liability for failure to comply with information	-	Employment contracts with employees provide for employees' liability for non-compliance with information security requirements

	liability after dismissal from the financial organization.	security requirements		
21.	Employees of a financial organization undergo training or retraining in order to regularly receive information on the requirements of rules and procedures for information security in a financial organization.	Employees are not trained on the requirements of rules and procedures for information security.	Training of employees about the requirements of rules and procedures for information security is carried out irregularly (less than once every six months over the last 3 years).	Employees are trained on the requirements of rules and procedures for information security on a regular basis (at least once every six months over the last 3 years).
22.	Financial organization approved a document defining disciplinary liability for violation of rules and procedures on information security	There is no document defining disciplinary responsibility for violation of rules and procedures for information security.	There is an approved document that defines disciplinary liability for violation of rules and procedures for information security.	-
23.	Financial organization provides control over the return of the assets by employees that are in their use upon dismissal from the financial organization.	There is no process for control over the return of assets of a financial organization upon dismissal of employees.	The process of control over the return of assets of a financial organization upon dismissal of employees is carried out manually.	The process of control over the return of assets of a financial organization upon dismissal of employees is partially or fully automated.
24.	Financial organization ensures the revoking of employees' access to information processing facilities upon dismissal.	There is no process of revoking employee’s access to information processing facilities upon dismissal.	The process of revoking employees' access to information processing facilities upon dismissal is carried out manually.	The process of revoking employee’s access to information processing facilities upon dismissal is partially or fully automated.
25.	In a financial organization, physical access to information processing facilities is provided only to authorized employees.	There is no process of limiting physical access to information processing facilities.	The process of limiting physical access to information processing facilities is carried out manually.	The process of limiting physical access to information processing facilities is partially or fully automated.
26.	In a financial organization, server equipment is located in dedicated premises with the provision of a microclimate recommended by the equipment manufacturer.	Server equipment is located in workers' offices.	Server equipment is located in separate rooms where the microclimate is maintained. Microclimate monitoring is not carried out.	Server equipment is located in separate rooms where the microclimate is maintained. Microclimate monitoring is carried out with the notification of responsible workers.
		There is no interference		

27.	In a financial organization, server equipment is provided with uninterrupted, interference-free power.	protection and no backup power supply for server equipment.	There is anti-interference protection and backup power up to 1 hour for server equipment.	There is anti-interference protection and backup power for more than 1 hour for server equipment.
28.	Financial organization protects communication channels that go beyond the physical security perimeter.	Communication channels are not protected.	Encryption of communication channels between stationary offices and devices of a financial organization is carried out.	Encryption of communication channels between stationary offices and devices of a financial organization, as well as communication channels with mobile devices of a financial organization is carried out.
29.	Financial organization destroys information from media before reusing it.	Destruction of information from media is not regulated and is not carried out.	Destruction of information from media is regulated and carried out by standard means of operating systems.	Destruction of information from media is regulated and carried out by specialized means of guaranteed destruction of information.
30.	Financial organization controls the movement of equipment across the physical security perimeter.	Control over the movement of equipment across the border of the physical security perimeter is not regulated and is not implemented.	Control over the movement of equipment across the border of the physical security perimeter is regulated and carried out in manual mode.	Control over the movement of equipment across the border of the physical security perimeter is regulated and automated, partially or fully.
31.	Financial organization has defined the rules for managing changes in key information systems.	The rules for managing changes in key information systems are not defined.	The rules for managing changes in key information systems have been defined; the change management process is carried out in manual mode.	The rules for managing changes in key information systems are defined; the change management process is partially or fully automated.
32.	Financial organization uses separate environments for the development, testing and industrial operation of key information systems.	Environments for development, testing and industrial operation of key information systems are not separated.	Environments for testing and industrial operation of key information systems are separated.	Environments for development, testing and industrial operation of key information systems are separated.
33.	In a financial organization, workers who develop changes to key information systems do not introduce them into an industrial environment.	Employees combine the responsibilities of developing and introducing changes in key	Responsibilities for development and introduction of changes in key information systems are divided between employees; developers' access to the industrial	Responsibilities for development and introduction of changes in key information systems are divided between employees;

		information systems.	environment is not limited.	developers have no access to the industrial environment.
34.	Financial organization installs and regularly updates software that detects malicious code, as well as checks computers and storage media for malicious code.	Malware detection software is not installed on all computers.	Software that detects malicious code is installed on all computers and is not regularly updated or scanned for malicious code on computers and storage media.	Software that detects malicious program code is installed on all computers; regular updates and scanning for the presence of malicious program code of computers and storage media are carried out.
35.	Financial organization regulates and implements processes for creation, verification and testing on a regular basis of backup copies of information and software of key information systems.	Backup copies of information and software of key information systems are not created.	Creation of backup copies of information and software of key information systems is regulated and carried out in accordance with the approved regulations. Backups are not tested.	Creation and testing of backup copies of information and software of key information systems is regulated and carried out in accordance with the approved regulations.
36.	Financial organization maintains and stores audit logs of key information systems, recording user actions, emergency situations and information security events, for use in future investigations and monitoring access control.	Keeping audit logs for key information systems is not regulated, audit logs are maintained with the "default" settings or not.	-	Maintaining, configuring and storing audit logs of key information systems are described in internal approved documents; audit logs are configured, maintained and stored in accordance with the approved documents.
37.	Financial organization ensures registration and regular analysis of the actions of privileged users in key information systems	Actions of privileged users in key information systems are not recorded.	Actions of privileged users in key information systems are recorded, but not analyzed on a periodic basis.	Actions of privileged users in key information systems are recorded and analyzed on a periodic basis.
38.	Financial organization synchronizes the system time of key information systems using a single source of accurate time.	The system time of key information systems within a financial organization is not synchronized.	-	The system time of key information systems within a financial organization is synchronized using a single source of accurate time
39.	In a financial organization, users' access to key information systems is carried out by unique personal identifiers.	No unique personal identifier is required to access one or more key information systems.	-	Access to all key information systems is carried out by unique personal identifiers.
	Financial organization uses the functionality of differentiating user access	Differentiation of user access levels is used		

40.	levels in key information systems.	not in all key information systems.	-	Differentiation of user access levels is used in all key information systems.
41.	Financial organization approved and communicated to all employees of the financial organization a document containing the rules for managing user passwords in key information systems.	There is no document containing the rules for managing user passwords in key information systems.	-	There is an approved document containing the rules for managing user passwords in key information systems, communicated to all employees of the financial organization
42.	Financial organization approved and communicated to all employees of the financial organization a document containing the rules for periodic review of the current user access rights to key information systems.	There is no document containing the rules for periodic review of the current user access rights to key information systems	-	There is an approved document containing the rules for periodic review of the current user access rights to key information systems.
43.	Financial organization uses two- or multi-factor authentication to connect users outside the physical security perimeter.	To connect users from outside the physical security perimeter, one factor is used for authentication.		Users connect from outside the physical security perimeter using two- or multi-factor authentication.
44.	The information network of a financial organization is delimited into groups (VLAN) .	Delimitation of the information network of a financial organization into groups is not provided.	The information network of a financial organization is delimited into groups according to the functional characteristics of information processing facilities.	The information network of a financial organization is delimited into groups based on the classification of the processed information.
45.	Financial organization uses the functionality of automated password management in key information systems.	Functionality of automated password management is not used in key information systems.	Key information systems use the functionality of self-changing passwords by users, control of periodic password changes.	Key information systems use the functionality of self-changing passwords by users, control of periodic password changes, control of password complexity, control of repeating previous passwords.
46.	Financial organization approved and communicated to all employees of the financial organization a document containing the rules for working in a remote mode.	There is no document containing the rules for working in a remote mode	-	There is an approved document containing the rules for working in a remote mode, brought to the attention of all employees of the financial organization.

47.	Financial organization approved and communicated to all employees of the financial organization a document containing the rules for the use of cryptographic information protection tools	There is no document containing the rules for the use of cryptographic information protection tools	-	There is an approved document containing the rules for the use of cryptographic information protection tools, brought to the attention of all employees of a financial organization who have access to cryptographic information protection tools.
48.	Financial organization approved and communicated to all employees of the financial organization a document containing the rules for managing cryptographic keys.	There is no document containing the rules for managing cryptographic keys	-	An approved document is available containing the rules for managing cryptographic keys.
49.	Financial organization provides control over access to the source codes of key information systems.	Access to the source codes of key information systems is not limited	Access to the source codes of key information systems is provided only to developers.	Access to the source codes of key information systems is provided only to developers, information about all changes in the source codes is automatically recorded in the log.
50.	Financial organization analyzes information on technical vulnerabilities of key information systems, assesses the severity of such vulnerabilities and takes measures to eliminate them.	Analysis of information on technical vulnerabilities of key information systems is not carried out.	-	Periodic analysis of information on technical vulnerabilities of key information systems is carried out, the danger of such vulnerabilities is assessed and measures are taken to eliminate them.
51.	Employees of the financial organization are notified of the need for immediate notification of any noticed or suspected information security breaches.	There is no process for notifying employees about the need to report on information security breaches	Employees are periodically notified of the need to report on information security breaches.	Employees are periodically notified of the need to report on information security breaches, and periodic checks of employees' actions are carried out when information security breaches are detected.
52.	Financial organization has approved a document containing procedures for responding to information security incidents.	There is no document containing procedures for responding to information security incidents	-	An approved document containing procedures for responding to information security incidents is available
53.	Financial organization keeps a record of information security incidents and their subsequent analysis.	Information security incidents are not recorded.	Information security incidents are registered, no analysis has been carried out over the past year.	Information security incidents are registered, the results of the analysis over the past year are documented.

54.	Financial organization provides regular penetration testing of the information infrastructure.	Penetration testing of the financial organization's information infrastructure is not carried out.	Penetration testing of the information infrastructure of a financial organization is carried out less than once a year.	Penetration testing of the information infrastructure of a financial organization is carried out at least once a year.
55.	Financial organization regularly analyzes the vulnerabilities of the source codes of key information systems if there is access to such source codes.	Analysis of the source codes of key information systems for vulnerabilities is not carried out.	Analysis of the source codes of key information systems for vulnerabilities is carried out selectively, not for every change in the industrial environment.	Analysis of the source codes of key information systems for vulnerabilities is carried out before each change in the industrial environment.