Approved by
Chairman of the Board, Rector of
Abylkas Saginov Karaganda Technical University NJSC
_____ S.S. Sagintayeva
Board decision
No. 29 dated JANUARY 14 2026

INTERNAL REGULATORY DOCUMENT

METHODOLOGY OF INFORMATION SECURITY RISK ASSESSMENT

IRD II-01-2026

Developed by: Information security engineer
D.K. Chityan_____

Karaganda

Contents

1 Scope

1.1 This Methodology of information security risk assessment (hereinafter referred to as the Methodology) of Abylkas Saginov Karaganda Technical University NJSC (hereinafter referred to as the University) was developed to implement the requirements of the University Information Security Management System and is applied in accordance with the current legislation of the Republic of Kazakhstan, national and international information security standards, and the University's internal regulatory documents.

1.2 The Methodology establishes a unified approach to the identification, analysis, assessment, processing, and monitoring of information security risks associated with the University's assets within the scope of the Information Security Management System.

1.3 The provisions of this Methodology apply to all the information assets of the University, including information, information systems, software, computing equipment, and other information processing tools, regardless of their presentation form, storage method, and transmission method.

1.4 The requirements of the Methodology are mandatory for all the structural divisions, University employees, asset owners, risk owners, and other persons involved in information security risk management processes or having access to assets within the scope of the Information Security Management System.

1.5 The Methodology is applied in the design, implementation, operation, modernization, and decommissioning of information systems, as well as in conducting internal audits, analyzing information security incidents, and making management decisions in the field of information security.

2 Regulatory references

2.1 The following regulatory documents were used in developing the Methodology:

1) Law of the Republic of Kazakhstan dated November 24, 2015, No. 418-V "On Informatization".

2) ST RK ISO/IEC 27002-2023 “Information security, cybersecurity and privacy protection. Information security controls”.

3) ST RK ISO/IEC 27001-2023 “Information security, cybersecurity and privacy protection. Information security management systems. Requirements”.

4) Resolution of the Government of the Republic of Kazakhstan dated December 20, 2016, No. 832 "On Approval of Uniform Requirements in the Field of Information and Communication Technologies and Information Security".

2.2 The Methodology is an internal regulatory document of the University and complies with the University Information Security Policy.

3 Terms, definitions and abbreviations

3.1 The following abbreviations and key concepts are used in this Methodology:

1) University – Abylkas Saginov Karaganda Technical University NJSC;

2) Methodology – Methodology of Information Security Risk Assessment;

3) Residual risk – the risk that exists given the current preventive measures and risk response measures should they materialize;

4) Risk owner – the person (employee/department/authorized body) responsible for all aspects of managing a specific risk, in particular, reducing the likelihood of the risk materializing and/or reducing the possible impact of the risk materializing on the University;

5) ISMS – the University Information Security Management System;

6) Assets – information of value to the University, in accordance with the scope of the ISMS, as well as information processing tools;

7) Asset owner – the University employee or department assigned administrative responsibility for the ISMS asset.

4 Responsibility and authority

4.1 The Information Security Service organizes and coordinates the risk assessment process, provides methodological support for the application of the Methodology, monitors the correctness of risk identification, analysis, and treatment, compiles consolidated results, and presents them to management.

4.2 Asset owners are responsible for ensuring the asset inventory is up-to-date, participating in the identification of threats and vulnerabilities, implementing protective measures, and providing reliable information for risk assessment.

4.3 Risk owners decide on risk treatment methods, are responsible for the level of residual risk, and implement risk management measures within the approved acceptance criteria.

4.4 Heads of structural divisions ensure employee participation in risk assessment procedures and the implementation of risk treatment measures.

4.5 University employees are obligated to comply with the requirements of the Methodology and participate in risk identification and analysis processes within the scope of their job responsibilities.

5 General provisions

5.1 The Information Security Risk Assessment Methodology guides University employees in the process of risk identification and assessment.

5.2 The purpose of the Methodology is to identify risks, to determine their key characteristics, and to determine the level of their threat to the availability, integrity, and confidentiality of ISMS assets and the achievement of established objectives over a specified period of time.

5.3 Asset owners participate in risk identification to increase the likelihood of identifying all risks and obtaining an objective assessment and level of risk impact on established objectives.

6 Procedure for identification, analysis and assessment of risks

6.1 To identify risks, it is necessary to formulate the key objectives and goals facing the employees for whom they are responsible, and the University as a whole, and to identify the threats/risks that affect or may affect the successful achievement of the stated ISMS goals and objectives. This process results in the compilation of a list of potential risks, including those arising from vulnerabilities in the University's information assets.

6.2 After identifying the list of risks, it is necessary to determine their main characteristics, indicate the possible causes of each risk, and describe the possible consequences if it materializes.

6.3 The main characteristics of a risk include its initial assessment, existing preventive measures within the risk response plan and an assessment of their effectiveness, an action plan in the event of a risk materialization and an assessment of its effectiveness, an assessment of the residual risk, the assignment of a risk owner, and an indication of the frequency of risk audits.

6.4 To assess each risk and the effectiveness of risk response measures, a scoring method is used. This method involves assigning specific numerical values to the corresponding qualitative characteristics and allows for the creation of a quantitative risk assessment.

6.5 Initial risk assessment allows for the evaluation and determination of the risk's significance without taking into account any existing response measures by assessing two risk parameters: the likelihood of risk occurrence and the degree of impact of negative consequences should it occur.

6.6 The likelihood of risk occurrence is assessed on a scale of 1 to 5, depending on the risk's past frequency or qualitative characteristics. To determine the appropriate score, the values for each score are presented in the following table:

Score	Probability	Quality characteristic	Quantity characteristic
5	Very high	The probability of risk occurrence is extremely high. There is a history of this risk occurring multiple times. The risk has occurred in the recent past.	Once a month
4	High	The probability of risk occurrence is high. There is a history of this risk occurring multiple times.	Once a quarter
3	Medium	The risk may occur. There is a history of this risk occurring.	Once every six months
2	Low	The probability of risk occurrence is low. The risk has never occurred before. However, the risk requires monitoring, as its occurrence is possible under certain conditions.	Once a year
1	Very low	The probability of risk occurrence is extremely low. The risk has never occurred before. However, the risk requires monitoring, as its occurrence may increase under certain conditions.	Once every 3 or more years

6.7 The impact of negative consequences in the event of a risk being realized is assessed based on the description of the degree of possible consequences, which are defined in the following table:

Score	Degree of influence	Description
5	Critical	If the risk is realized, the University will be virtually unable to fully recover from the consequences associated with this risk.
4	Significant	The consequences of the risk are very significant, but can be mitigated to a certain extent.
3	Moderate	The consequences of the risk are significant, but can be fully mitigated.
2	Low	The consequences of the risk are minor.
1	Extremely minor	There are no consequences if the risk is realized.

6.8 After conducting the initial assessment, it is necessary to indicate the existing preventive measures for each risk that are in place at the University to prevent the realization of this risk, and also to indicate the corresponding specific person responsible for this measure.

6.9 As part of monitoring the effectiveness of risk management methods, existing risk prevention measures should be assessed to determine the need for improvement.

When assessing the effectiveness of preventive actions, the following scale should

be used:

Score	Description
1	Preventive measures are effective and comparable to international best practices used by other companies in similar fields.
2	Control measures are highly effective and exceed the minimum level of measures established by regulatory authorities. Company employees are confident in the effectiveness of these measures.
3	Preventive measures are rated at an average level; their effectiveness is sufficient to prevent incidents or reduce the impact of incidents to an acceptable level. They meet minimum regulatory requirements.
4	Some control measures exist, but they are likely ineffective and outdated, having only a minor impact on incident prevention.
5	Preventive measures are absent.

6.10 As a result of setting the risk characteristics, an overall risk rating is assigned based on the initial risk assessment and existing preventive measures (risk rating 1), which is calculated using the following formula:

Rating of risk 1 = Assessing the likelihood of risk occurrence *
Assessing the impact of negative consequences if the risk occurs *
Assessing the effectiveness of preventive actions

At this,

- the risk probability assessment is specified in accordance with Section 3.6 of the Methodology,
- the impact of negative consequences in the event of risk realization is assessed in accordance with Section 3.7 of the Methodology,
- the effectiveness of preventive actions is assessed in accordance with Section 3.9 of the Methodology.

6.11 The definitions of the digital expression of risk rating 1 are given in the following table:

Designation	Risk total significance	Definition
Over 40	Very high	Risk responses must be defined or, if any, improved, and prepared for implementation before the start of project/task implementation or immediately after risk identification during project/task implementation.
30-39	High	Risk responses must be defined or, if any, improved, and implemented promptly during project/task implementation.
20-29	Medium	Risk responses must be defined or, if any, improved within the established optimal timeframes and implemented during project/task implementation.
10-19	Low	Risks in this category must be controlled, but preparation of response measures is not required.
Under 10	Very low	Preparation of response measures is not required.

6.12 When describing the risk characteristics, the existing measures/established actions to be taken in the event of a risk occurrence should be indicated, as well as the person responsible for this measure, if the risk rating value of 1 is above average, i.e., above 30. In this case, an assessment of the action plan in the event of a risk occurrence should be carried out in order to determine the effectiveness of existing risk management methods and identify the need for their improvement. For these purposes, the following scale should be used:

Score	Description
1	Risk response measures are effective and comparable to global best practices used by other companies in similar industries.
2	Risk response measures are highly effective and exceed the minimum level of measures established by regulatory authorities. Company employees are confident in the effectiveness of these measures.
3	Risk response measures are rated as average; their effectiveness is sufficient to prevent significant losses. They comply with minimum regulatory requirements.
4	Some risk response measures exist, but they are likely ineffective and outdated, with only a limited impact on loss prevention.
5	There are no risk response measures.

6.13 If the risk rating value of risk 1 is equal to or below the average level (below 30), it is necessary to assign an assessment of the effectiveness of actions in the event of risk realization at the level of assessment of the effectiveness of preventive actions, guided by the scale presented in section 3.9.

6.14 Re-risk assessment is conducted taking into account existing risk response measures, thereby determining the level of residual risk. During the initial assessment, the risk itself was assessed; at this stage, the risk is assessed taking into account existing risk response plans, i.e., risk management methods.

6.15 The point scale for assessing the risk impact and the likelihood of risk realization during the residual risk assessment corresponds to the scale for the initial risk assessment specified in sections 3.6 and 3.7 of the Methodology, respectively.

6.16 As a result of entering all the above risk characteristics, an overall risk rating is assigned, based on the re-risk assessment and existing preventive measures, and also, if necessary, taking into account the action plan in the event of risk realization (risk rating 2), which is calculated using the following formula:

Rating of risk 2 = Assessing the likelihood of risk occurrence *
Assessing the impact of negative consequences if the risk occurs *
Assessing the effectiveness of the action plan if the risk occurs (or assessing the effectiveness of preventive actions if the risk rating is below 30).

6.17 The definitions of the digital expression of risk rating 2 are given in the following table:

Designation	Risk total significance	Description
Over 40	Very high	Risk response measures must be defined or, if any, improved, and prepared for implementation before the start of project/task implementation or immediately after the risk is identified during project/task implementation. An action plan must be promptly prepared or improved in the event of a risk realization.
30-39	High	Risk response measures must be defined or, if any, improved, and implemented during project/task implementation. An action plan must be promptly prepared or improved in the event of a risk realization.
20-29	Medium	Risk response measures must be defined or, if any, improved within the established optimal timeframes and implemented during project/task implementation.
10-19	Low	Risks in this category must be controlled, but the preparation of response measures is not required.
Under 10	Very low	The preparation of response measures is not required.

The final characteristics of the risk are the indication of the risk owner and the frequency of audit/revising the risk status.

7 Coordination, approval and implementation

7.1 This Methodology is subject to approval by the heads of the University structural divisions whose activities are related to the ownership and operation of information assets. If the provisions of the Methodology affect issues of strategic management, resource allocation, or management decision-making, approval is obtained from the relevant authorized divisions.

7.2 The list of officials with whom the Methodology must be approved is determined by the document developer, taking into account its content, scope of application, and impact on the processes of the information security management system.

7.3 The review period for the draft Methodology should not exceed five business days from the date of its receipt. Comments and suggestions must be presented in a reasoned and specific manner.

7.4 If there are no comments, or after they have been taken into account, the Methodology is signed by the approving officials and submitted for approval to the executive body, the Management Board.

7.5 The date of its approval is considered the date of entry into force of the Methodology. From the date of approval, the Methodology is mandatory for application.

7.6 When a new version of the Methodology is approved or amendments are made, the previous version becomes invalid and is considered void.

8 Safekeeping

8.1 The original of this Methodology is stored in the University Information Security Service.

8.2 An electronic version of the Methodology is posted on the University's corporate information resources, ensuring access for interested structural divisions and employees involved in information security risk management processes.

8.3 University employees are familiarized with the Methodology in accordance with the procedure established for internal regulatory documents, with the completion of an familiarization sheet.

8.4 The heads of the relevant divisions are responsible for maintaining records of copies of the Methodology, preventing its unauthorized use, and maintaining its safekeeping within the structural divisions.

9 Procedure for revising and updating

9.1 This Methodology is reviewed by the Information Security Service at least once every two years and is aimed at aligning the applied risk assessment approaches with the current operating conditions of the University, the development of information technology, and the requirements of the Information Security Management System.

9.2 Unscheduled updates of the Methodology are carried out in the event of changes in the scope of the Information Security Management System, changes in the requirements of the legislation of the Republic of Kazakhstan and international information security standards, the implementation of new information systems, significant infrastructure upgrades, as well as based on the results of internal audits, analysis of information security incidents, and risk management effectiveness assessments.

9.3 Amendments and additions to this Methodology are documented as a new version or a separate administrative document and are approved in accordance with the procedure established for approval of the Methodology.

Appendix 1
to the Methodology of information security risk assessment

RULES
of identifying information security risks

1 General provisions

1.1 These Rules of risk identification been developed in accordance with the other internal documents of Abylkas Saginov Karaganda Technical University NJSC " (hereinafter referred to as the University).

1.2 The Rules of risk identification (hereinafter referred to as the Rules) define the procedure, methodology, and identification and assessment of risks, as well as the control of current risks and monitoring the effectiveness of risk management methods on a consolidated basis.

1.3 Risk identification is performed to obtain an overview of risks and their main characteristics, determine the interrelationships between risks, rank risk levels, and increase awareness of risks and risk management methods in order to identify the most critical risks and take measures to manage them.

1.4 Risk identification is a tool for recording and reporting potential negative events that may adversely affect the achievement of the goals and objectives set for the University and each of its employees, as well as determining the direction and need for improvement of the risk management process.

1.5 Compliance with these Rules is mandatory for all University employees.

2 Additional terms used in the Rules

2.1 The following abbreviations and key concepts are used in these Rules:

1) Residual Risk – the risk that exists taking into account current preventive measures and risk response measures should they occur.

2) Risk Owner – the person (employee/department/authorized body) responsible for all aspects of managing a specific risk, in particular, reducing the likelihood of risk occurrence and/or reducing the possible impact of the risk's consequences on the University.

3) ISMS – the University Information Security Management System.

4) Assets – information of value to the University, according to the scope of the ISMS, as well as information processing tools.

5) Asset Owner – the University employee or department assigned administrative responsibility for the ISMS asset.

6) DIT – Department of Information Technology.

7) ISS – Information Security Service

3 Procedure for conducting risk identification and assessment within the planned monitoring

3.1 An employee of the Information Technology Department (hereinafter referred to as the DIT), in collaboration with the owners of the University assets, continuously identifies and assesses risks affecting the availability, integrity, and confidentiality of the ISMS Assets. This process is carried out through the annual completion of a risk map, in accordance with Appendix No. 1 to the Rules.

3.2 When completing the risk map, University employees are guided by the University's Information Security Risk Assessment Methodology.

3.3 Completed risk maps are submitted to Chairman of the Management Board, Rector no later than 5 (five) business days before the end of the reporting period.

3.4 The Executive Body takes note of the information on risks identified by employees, analyzes it, and instructs the Information Security Officer (hereinafter referred to as the ISO) to compile a consolidated risk map.

3.5 The University ISS analyzes the risk information and prepares a consolidated risk map for the University. If necessary, the ISS can request information necessary for a more complete disclosure of the identified risks.

3.6 The University's risk summary map is sent to Chairman of the Management Board, Rector of the University no later than five (5) business days after the reporting period.

3.7 Based on the risk summary map, the University's Information Security Department prepares a brief report on the main ISMS risks, which is submitted to the executive body for review. This report includes information on the results of the risk ranking conducted as part of the risk map, existing measures to respond to critical risks, indicating their effectiveness, and proposals and an action plan for improvement.

4 Procedure for conducting identification of new risks

4.1 In the event of a new risk being identified or a negative change in the status of an existing risk, the owner of the University asset registers or changes the risk status by amending the existing risk map immediately after such discovery.

4.2 After processing the information received, the University Information Security Department submits a report and a plan for managing the identified risk to management.

5 Control over current risks and monitoring the effectiveness of risk management methods

5.1 The Information Security Service (ISS) continuously monitors current risks and the effectiveness of risk management methods.

5.2 Risk management methods are improved based on the results of risk identification.

5.3 Responsibility for organizing the risk identification and assessment process rests with the ISS.

5.4 Responsibility for compliance with the requirements of these Rules rests with the Asset owners and the University Information Security Officer.

5.5 Responsibility for developing the Risk Management Process Improvement Plan rests with the ISS.

Appendix 2
to the Methodology of
information security risk assessment

List and assessment of ISMS risks

Risk owner				**Risk primary assessment**		**Primary assessment taking into account the existing preventive measures**				**Plan of activities to respond risks (preventive measures)**			**Repeated risk assessment after taking measures to reduce the probability of occurrence (residual risk)**				
Risk number	**Risk or threat name**	**Reasons for risk occurrence**	**Description of possible consequences of risk implementation**	**Probability of risk implementation (from 1 to 5)**	**Assessment of possible negative consequences of risk implementation (from 1 to 5)**	**Preventive actions**	**Person or structural division responsible for actions**	**Assessment of preventive measures effectiveness**	**Risk rating**	**Measures to reduce probability of risk implementation**	**Person or structural division responsible for actions**	**Assessment of effectiveness of preventive measures after actions to reduce risk**	**Probability of risk implementation (from 1 to 5)**	**Assessment of influence, possible negative consequences after risk implementation (from 1 to 5)**	**Rating of risk 1**	**Risk owner**	**Periodicity of revision**
1																	
2																	
3																	

Information security service:

_____
(name, position, signature)

_____
(name, position, signature)

Appendix 3
to the Methodology of
information security risk assessment

List and assessment of ISMS risks, continued

Risk owner				**Risk primary assessment**		**Primary assessment taking into account the existing preventive measures**				**Plan of activities to respond risks (preventive measures)**			**Repeated risk assessment after taking measures to reduce the probability of occurrence (residual risk)**				
Risk number	**Risk or threat name**	**Reasons for risk occurrence**	**Description of possible consequences of risk implementation**	**Probability of risk implementation (from 1 to 5)**	**Assessment of possible negative consequences of risk implementation (from 1 to 5)**	**Preventive actions**	**Person or structural division responsible for actions**	**Assessment of preventive measures effectiveness**	**Risk rating**	**Measures to reduce probability of risk implementation**	**Person or structural division responsible for actions**	**Assessment of effectiveness of preventive measures after actions to reduce risk**	**Probability of risk implementation (from 1 to 5)**	**Assessment of influence, possible negative consequences after risk implementation (from 1 to 5)**	**Rating of risk 1**	**Risk owner**	**Periodicity of revision**
1																	
2																	
3																	

Information security service:

_____
(name, position, signature)

_____
(name, position, signature)

F.01-2022

Coordination sheet

Position	Name	Date	Signature
Member of the Board, Vice-rector for Digitalization	Amirov A.Zh.	9.12.25	
Member of the Board, Vice-rector for Strategic Development and Internationalization	Kanapyanov T.E.	9.12.25	
Head of the Legal Service	Ayazbayeva G.S.	9.12.25	
Head of the Sustainable Development Center	Shebalina O.A.	9.12.25	

F.02-2022

Familiarization sheet

Position	Name	Date	Signature