Poznan University of Medical Sciences

DOP-140/21

Decree No 55/21
of the Rector of Poznan University of Medical Sciences of 26 April 2021

regarding the establishment of "Procedure of the system of management control and risk management at the Poznan University of Medical Sciences".

Pursuant to § 28(1) of the Statute of the Poznan University of Medical Sciences in conjunction with Article 69(1)(3) of the Act of 27 August 2009 on Public Finance (Journal of Laws of 2021.305), it is decreed as follows:

§ 1

The "Procedures of the management control system and risk management at the Poznan University of Medical Sciences" are established, which constitute Appendix 1 to the present Regulation.

§ 2

The Director General is entrusted with the execution of the decree.

§ 3

The decree shall come into force as of the date of its signing, effective as of 1 January 2021. At the same time, Decree No 19/21 of the Rector of the Poznan University of Medical Sciences of 4 March 2021 on establishing "The procedure of the system of management control and risk management at the Poznan University of Medical Sciences" shall expire.

Rector

Prof. Andrzej Tykarski, MD, PhD

Appendix 1 to Decree No 55/21 of 26 April 2021

PROCEDURE OF THE SYSTEM OF MANAGEMENT CONTROL AND RISK MANAGEMENT AT THE POZNAN UNIVERSITY OF MEDICAL SCIENCES

§ 1

Management control and risk management at the Poznan University of Medical Sciences, hereinafter referred to as the University, constitutes a set of actions taken by the Rector, Vice Rectors, Chancellors of Colleges, Directors, Deans of Faculties, Heads of Comprehensive Units, Heads of organizational units, as well as other employees in order to ensure the implementation of objectives and tasks in a legal, effective, economical and timely manner.

§ 2

The purpose of management control is to ensure at the University:

1) compliance of activities with legal regulations and internal procedures;
2) effectiveness and efficiency of activities in the performance of tasks through economical and efficient use of personnel, property and material resources;
3) reliability of reports;
4) protection of resources by securing assets against destruction, loss and embezzlement, and personal data and classified information;
5) adherence to and promotion of ethical conduct;
6) efficiency and effectiveness of the flow of information necessary to perform official duties and effective internal and external communications;
7) risk management to increase the probability of achieving goals and tasks by preventing unfavorable phenomena in the University's activities, indicating ways and means to prevent the emergence of irregularities and their elimination.

§ 3

1. The purpose of risk management is to reduce risk as much as possible and to protect the University from its negative effects, as well as activities that increase the probability of achieving the assumed objectives.
2. The implementation of risk management procedures is intended to:
   1) provide a systemic framework through which activities are conducted in a consistent and controlled manner;
   2) improve decision making, planning and prioritization;
   3) protect and build the image of the Medical University;
   4) develop knowledge capacity;
   5) improve operational efficiency;
   6) improve the quality of service delivery;
   7) effectively manage projects;
   8) provide controls in proportion to risk;
   9) ensure principles of integrity and economy that prevent fraud and waste of property.

§ 4

1. The person responsible for ensuring the operation of adequate, effective and efficient management

control is the Rector and the Director General.

2. Responsibility for the functioning of an adequate system of management control within the scope of their competence and tasks is also borne by Vice Rectors, Chancellors of Colleges, Directors, Deans of Faculties, Heads of Comprehensive Units, Heads of organizational units.
3. The assessment of the management control system is performed by the Internal Auditor during the audit tasks.
4. Under the authority of the Rector, supervision of the management control system and risk management is exercised by the Director General.

§ 5

1. Risk management is carried out in two stages:
   1) at the strategic level it refers to the annual identification and analysis of risks;
   2) at the operational level it refers to the ongoing identification, assessment of risks and taking remedial action.
2. Responsibility for risk management at the strategic level is held by the Rector through:
   1) shaping, implementing and overseeing the risk management procedure;
   2) identifying risk factors and assessing risks at the strategic level;
   3) determining the level of acceptable risk;
   4) promulgating and implementing risk management procedures, including monitoring the effectiveness of controls;
   5) designating risk owners during the strategic risk management phase.
3. Directors are involved in the process of identifying and assessing risks at the strategic level.
4. The Rector may assign responsibility for the management of key risks - relating to the University's main objectives - to the relevant Director.

§ 6

1. At the operational level, heads of administrative units are responsible for risk management through:
   1) identifying and documenting risk factors relevant to the achievement of operational objectives (Appendix 1), which shall occur one time after the effective date of this decree;
   2) assessment of the materiality of the risk factors in relation to the objectives pursued, taking into account the likelihood and potential impact of the risks caused by those factors (Appendix 2), which shall occur on a one-time basis after the entry into force of this decree;
   3) monitoring of the level of operational risk, including the functioning of control mechanisms in terms of their adequacy and effectiveness, as well as any deviations from the existing procedures and identification of possible newly arising risks, shall be carried out once a year, based on Appendix 1;
   4) designing remedial actions within the scope of its area of activity or submitting to its immediate supervisor written proposals for solutions that will contribute to reducing risks to an acceptable level;
   5) identifying and documenting data protection risk factors (Appendix 3) which occurs one time after the effective date of this decree;
   6) monitoring of the level of operational risk, including the functioning of control mechanisms in terms of their adequacy and effectiveness, as well as any deviations from the existing procedures and identification of possible newly arising risks, shall be carried out once a year, based on Appendix 3;
2. Heads of administrative units shall receive in electronic form the documents referred to in

paragraph 1.

§ 7

Management control in the University is carried out through:

1) self-control - control of the correctness of all employees' performance of their own work, in accordance with their scopes of duties;
2) functional control - control exercised as part of supervisory duties by employees in managerial positions;
3) preliminary control - control carried out before undertaking economic operations;
4) follow-up control - control conducted after the occurrence of the actual incident, aimed at detecting irregularities.

§ 8

Annual risk identification and analysis constitutes the basis for risk management (Appendix 1).

§ 9

The risk analysis includes the following steps:

1) identification of risks that may affect the achievement of the University's objectives;
2) evaluation of existing measures used to keep risks under control;
3) analysis and prioritization of risks according to impact and likelihood of risk occurrence;
4) defining the measures required to deal with unacceptable risks;
5) identification of persons in management responsible for taking remedial action and setting a deadline for taking action;
6) monitoring and reporting on actions taken.

§ 10

Risk identification at the University shall be performed at least once a year.

§ 11

The owner of the identified risk in each category is the Rector of the University.

§ 12

The identified risks should be subjected to analysis in order to determine the probability of occurrence of a given risk and to determine its consequences.

§ 13

For the purpose of determining the probability of a risk occurrence and its consequences, the scale specified in Appendix 2 is adopted.

§ 14

1. The level of acceptable risk for the risk identified and analyzed at the University is determined by the Rector or, under his authority, by the Director General.
2. The decision to accept any level of risk and not to take remedial action may be made by the Rector or under his authority by the Director General.
3. Having identified and analyzed the risks within the activities of their unit, the Heads of administrative units are required to prepare a risk statement (according to the templates specified in Appendix 1 and 4) and submit these documents to the Internal Auditor within the time specified by the Rector or the Director General.
4. Having collected the documents referred to in paragraph 3, a general risk list is drawn up and then forwarded to the Rector or to the Director General authorised by the Rector for approval.

§ 15

1. The risk monitoring process is continuous and should be performed at each management level as part of exercising management control.
2. Employees of the University have the right and duty to report to their superiors existing risks at their workstation and management supports employees' actions to minimize potential risks.
3. Assessment of how risks are managed is made by the Internal Auditor during audit assignments.
4. Employees of the University are required to follow the procedures in the Management Control and Risk Management System Procedure.

§ 16

1. In case of changes in legislation, organizational changes, imposition of additional tasks and occurrence of other important circumstances during the year, Heads of administrative units are obliged to take immediate action to identify and analyze risks and inform the Internal Auditor about it.
2. The Management Control and Risk Management System procedure is reviewed and updated on an ongoing basis as necessary.
3. Changes to the Management Control and Risk Management System Procedure are approved by the Rector.

Appendix 1 to the Procedure of the management control system and risk management

RISK REGISTER - CORE BUSINESS OF THE UNIVERSITY I												
Name of the organizational unit:			***POZNAN UNIVERSITY OF MEDICAL SCIENCES***									
item	areas of core activity of the university	subareas of the university's core business	risk name	risk number	probability of risk on the scale 1 - 4	effect (impact) of the risk on the scale 1 - 4	risk severity index	risk level	planned methods of risk counteracti on	describe the risk reduction measures	responsible entity	lead time
1	2	3	4	5	6	7	8	9	10	11	12	13
1.												
2.												

RISK REGISTER - SUPPORT ACTIVITIES OF THE UNIVERSITY II												
name of the organizational unit:			***POZNAN UNIVERSITY OF MEDICAL SCIENCES***									
item	areas of supporting activity of the university	subareas of activities supporting the university	risk name	risk number	probabili ty of risk on the scale 1 - 4	effect (impact) of the risk on the scale 1 - 4	risk severity index	risk level	planned methods of risk counteracti on	describe the risk reduction measures	responsible entity	lead time
1	2	3	4	5	6	7	8	9	10	11	12	13
1.												
2.												

Appendix 2 to the Procedure of the management control system and risk management

scale for assessment of probability and effect of risk occurrence		
effect	**scale**	**description**
very high	4	very high influence on implementation of the task and achievement of the assumed goal (making implementation of the goal impossible). The occurrence of an event covered by the risk involves a long and difficult process of restoring the previous state
high	3	significant impact on the implementation of the task and achievement of the objective. The occurrence of an event covered by the risk involves a long and difficult process of restoring the previous state
medium	2	moderate influence on the implementation of the task and achieving the assumed goal. The occurrence of an event covered by the risk involves a long and difficult process of restoring the previous state
low	1	low impact on the implementation of the task and achieving the assumed objective. Effects of the event can be easily removed
probability	**scale**	**description**
very high	4	happens more than once a year
high	3	happens once a year
medium	2	happens less than once a year
low	1	did not happen

Appendix 3 to the Procedure of the management control system and risk management

		Risk register - personal data of the higher education institution III									
	Name of the unit:	***POZNAN UNIVERSITY OF MEDICAL SCIENCES***									
	Name of the organizational unit:										
Item	**Risk name**	**risk number**	**present: yes no not applicable**	***complete these items (except for column 7 8) if you answered yes in column 4***							
				*rating scale							
				Probability of risk on the scale 1 - 4	**Effect (impact) of the risk on the scale 1 - 4**	**Risk severity index**	**Risk level**	**Planned methods of risk counteraction**	**Describe the risk reduction measures**	**responsible entity**	**lead time**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1.		III.1				0	LOW				
2.		III.2				0	LOW				

***scales for assessing the likelihood and impact of risks to personal data**		
effect	**scale**	**description**
very high	4	Significant or irreversible consequences for data subjects leading to physical harm or damage to property or non-property, in particular: if the processing is likely to result in discrimination, identity theft or identity fraud, financial loss, damage to reputation, breach of confidentiality of personal data protected by professional secrecy, or any other significant economic or social harm; if data subjects are likely to be deprived of their rights and freedoms or their ability to exercise control over their personal data. Threat to the continuation of operations, drastically disrupts or prevents work along with serious legal liability. Serious financial liability, including fines. Negative media publicity on a national scale.
high	3	Significant consequences for data subjects but resolvable with many difficulties. May disrupt work significantly with serious impact on operations. Legal liability is possible. Medium financial liability, including fines. Negative media publicity on a local scale.
medium	2	Minor consequences for data subjects and easily resolvable. Short-term, severe impact on operations, may disrupt work but can be restored by readily available means. Little financial liability, rather no or very low financial penalties.
low	1	Data subjects are not affected. No serious impact on operation, tasks can continue to be performed.
probability	**scale**	**description**
very high	4	happens more than once a year
high	3	happens once a year
medium	2	happens less than once a year
low	1	did not happen