BUDAPESTI
CORVINUS
EGYETEM

III. ECONOMIC REGULATIONS
III.15. Integrated Risk Management Regulation

At its meeting on 19 December 2016, the Senate supported the adoption of the University's Integrated Risk Management Regulation by its Resolution No. SZ-63/2016/2017 (19 December 2016) and, at the same time, the previous regulation ceased to apply.

AI-SZ/8/2017

I. General part

Pursuant to the provisions of Act CXCV of 2011 on Public Finances and in accordance with Government Decree No. 370/2011 (31 December) on the internal control system and internal audit of budgetary bodies, Corvinus University of Budapest (hereinafter referred to as: BCE or Institution) operates an internal control system to ensure the balance of public finances and the transparent, efficient and auditable financial management of public funds. The Chancellor is responsible for establishing, operating and developing an appropriate control environment, an integrated risk management system, control activities, an information and communication system and a monitoring system at all levels of the organisation, within the internal control system of the Institution.

The internal control system includes[1] the principles, procedures and internal regulations that ensure that

a) all activities and objectives of the budgetary body are consistent with the requirements of regularity, economy, efficiency and effectiveness,

b) no waste, misuse or misappropriation occurs in the financial management of assets and resources,

c) appropriate, accurate and up-to-date information is available on the functioning of the budgetary body, and

d) legislation on the harmonisation and alignment of the internal control system is implemented, taking into account the methodological guidelines.

The Institution has developed and operates its internal control system[2] in accordance with the guidelines and methodological recommendations published by the minister responsible for public finances.

The main objective of the management of the Institution is to ensure professional preparedness, impartiality and neutrality in the day-to-day work, to achieve moral integrity of public servants and to put public interest before individual interests in order to effectively combat corruption.

In carrying out its tasks as set out in its founding charter, the University strives to ensure that its financial management is transparent and open to public scrutiny. In the use of public funds, the principles of transparency and public scrutiny are at the heart of the issue, given that data on public funds and national assets are in the public interest.

1. § Governing legislation and professional materials

a) Act CXCV of 2011 on Public Finances;

b) Government Decree No. 368/2011 (31 December) on the implementation of the Act on Public Finances;

c) Government Decree No. 370/2011 (31 December) on the internal control system and internal audit of budgetary bodies;

[1] Government Decree No. 370/2011 (31 December) on the internal control system and internal audit of budgetary bodies
[2] Regulation on the Internal Control System of Corvinus University of Budapest

d) Internal Control Standards;

e) Internal Control Manual;

f) A methodological guide for the design of a control environment and an integrated risk management system (October 2016);

g) Methodological guide for receiving and investigating reports of incidents that breach organisational integrity (October 2016)

II. Introduction

1. § The purpose of the Regulation

By implementing this Regulation, we believe that we are contributing to the legal compliance of our internal control system and that the controls we have put in place ensure that risks are managed, contribute to the achievement of our objectives and strengthen the integrity of the organisation.

Given that budgetary bodies are required to operate an integrated risk management system, this Regulation defines the procedures for institutional risk management, the responsibilities and reporting lines, and the coordination and harmonisation of the task. The BCE's risk management identifies the risks inherent in the activities and financial management of the budgetary body, and defines the measures to be taken in relation to each risk and the way to monitor their implementation.

The main purpose of this Regulation is to provide a framework for the risk management processes, where processes, responsibilities, contributors and contact persons are defined, so that the risks that may adversely affect the activities of Corvinus University of Budapest or hinder the implementation of our strategy are addressed in the context of the risk management function.

2. § Scope of the Regulation

The personal scope of the Regulation covers:

a) the organisational units specified in the University's ROO;

b) persons who are in a public servant or additional employment relationship with the University (in particular: lecturers, Professor Emeritus/Emerita, supervisors of doctoral schools, persons employed under student contracts);

c) persons who are doctoral candidates at the University;

d) persons who have a student status with the University;

e) legal and non-legal persons having a civil law relationship with the University.

The material scope of this Regulation covers the risk management tasks performed in the framework of all the activities defined in the founding charter.

3. § Key concepts

- **Uncertainty:** in common parlance, it means that somewhere, sometime in the future, different events may occur, which can be both positive and negative. Uncertainty, like risk, is also an event that may occur in the future. It also means a lack of information.
- **Effectiveness:** the requirement that the objectives set are achieved, taking into account agreed modifications and changing circumstances, and that the difference between the planned and actual impact of the activity is as small as possible, or that the actual impact is better than planned.
- **Economy:** the requirement that the expenditure or inputs associated with the use of resources should be the lowest possible, while maintaining the quality specified by law or generally expected.
- **Efficiency:** the requirement that the value of the goods produced, services provided, other outputs of the task performed, or the income from them, exceeds as far as possible the expenditure or inputs associated with the resources used.
- **Shortcoming:** something that exists in every case, is factually verifiable and relates to the present. A problem indicates a fact or circumstance, a shortcoming describes a state.
- **Action plan:** a timetable for the implementation of measures prepared by the controlled organisation or organisational unit on the basis of the control recommendations, indicating the persons responsible for their implementation and the relevant deadlines.
- **Integrated risk management system:** a process-based risk management system that covers all the organisation's activities, ensures that the organisation's risks are fully identified, assessed against defined criteria, and that an action plan for managing risks is prepared and monitored, using a consistent methodology and procedures, taking into account the organisation's objectives and values.
- **Integrity:** Acting in accordance with social and professional norms in the performance of public duties; the proper functioning of a public administration body in accordance with the objectives, values and principles set by the head of the administrative organisation and the governing body.
- **Integrity management system:** a functional subsystem of the governance and management system that ensures the unity of the organisational culture by coordinating the activities of the persons and groups involved in the creation of the integrity-based operation of the public administration body, in line with the control environment defined in Government Decree No. 370/2011 (31 December) on the internal control system and internal audit of budgetary bodies (hereinafter referred to using the Hungarian abbreviation, Bkr.), by defining values, principles, objectives and rules, providing guidance and advice on how to follow them, monitoring compliance and enforcing it where necessary.
- **Integrity risk:** the possibility of misuse, irregularities or other events that may violate or compromise the objectives, values or principles of the public administration body.

- **Risk:** an event that is not precisely foreseeable, but with a non-negligible chance of occurring by chance, i.e. an event that has not yet occurred. An important additional characteristic of risk is that it is always related to the objectives of the organisation, as it reduces or prevents the possibility of achieving them.
- **Risk analysis:** an objective method for selecting the areas to be controlled, identifying the risks inherent in the activities and internal control systems of the budgetary body.
- **Risk factors:** considered as the root causes of risks, they are generally characterised as factors that generate risks, and, as a compounding effect of several risk factors, either increase the likelihood of risks occurring or increase their impact, in the worst case both.
- **Corruption:** "The violation or compromising of integrity in the performance of public duties by bribery or advantage" (Oxford English Dictionary).
- **Corruption risk:** an integrity risk that represents the possibility of an act of corruption occurring.
- **Problem:** refers to the present, so in this regulatory environment the problem is not called a risk, because when the problem arises it is already present in the life of the organisation. Problems usually become risk factors.
- **Irregularity:** a deviation from an existing rule. The concept of irregularities is very broad, covering both correctable omissions or shortcomings and acts that give rise to disciplinary, criminal, infringement or compensation proceedings.
- **Threat:** a risk that negatively affects the strategic/organisational objectives of the institution. There are positive risks, i.e. opportunities.
- **Abuse:** in the case of abuse of a right, it appears to be the exercise of a right, a legitimate conduct, but in reality it is a violation of the principle of the proper exercise of rights, an unlawful conduct because of the purpose and therefore prohibited.

4. § Person responsible for risk management

On the basis of the provisions already set out in the Regulation on the Internal Control System of the Institution: "…Within the framework of the university risk management system established in accordance with the provisions of the Bkr., the University pays special attention to the assessment and identification of integrity and corruption risks in connection with its operations and the management of the related risks…The assessment and collection of risks related to the University's activities also draws on the experience of staff members and executives who are involved in these activities on a day-to-day basis, as they actively contribute to the preparation of the assessment process. Once the risks have been assessed, the risk factors identified in each area and how to manage them will be communicated to the staff members working there…"

To ensure the proper implementation of the integrated risk management activity, the **Chancellor** will provide professional assistance by appointing a risk management coordinator, where process owners are obliged to cooperate with the person appointed to coordinate the integrated risk management system.

The **Risk Management Coordinator** is responsible for defining the framework of the integrated risk management system and for establishing and properly regulating the processes to ensure that the overall risk management functions of the University are implemented at the legal level. The Coordinator's role is to help the Risk Management Committee to move from a routine mode of communication that is competitive, in line with technical coordination, arguing with each other's ideas, to a cooperative mode of communication that is connected, aligned and intertwined with each other's ideas, i.e. a real dialogue. The Risk Management Coordinator is responsible for organising and managing the identification of risks in groups.

The main objective in the design of integrated risk management processes is to ensure that the risk management activities carried out in practice as part of daily routine tasks are documented and properly managed, and that reviews are carried out at specified intervals.

Process owners assess risks along the established risk processes.

The members of the **Risk Management Committee** define the risk universe and categorise the identified risks, then aggregate the assessments using a risk map.

As part of its assurance activities, the **internal auditor** assesses the organisation's risk management system and makes recommendations for its improvement. In its advisory role, it supports risk analysis. And as the process owner of internal control, it identifies and assesses the risks in its own process, and makes recommendations to mitigate those risks.

III. The risk management process

1. § Risk identification and assessment

The purpose of a risk assessment is to **define the risk universe** and rank its elements in terms of the likelihood and impact of risks.

In all cases, risks must be identified in relation to the organisational objectives, for the organisation as a whole and for individual processes. When identifying risks, the inherent risks must be identified. The identification of risks should be carried out along the established processes, but, in addition to identifying the risks in the processes, risks to the organisation as a whole should also be identified.

The risks should be formulated to include the cause of the event, the impact of the event and the organisational purpose affected by the event.

a) We distinguish between risks:

- inherent risk: which is the risk of irregularities or errors in the achievement of organisational objectives;
- audit risk: risk arising from the failure to prevent inherent risk factors and the occurrence of inherent risks not detected by the internal control embedded in the process;

- control risk: the internal control system of the budgetary body is not able, through its own fault, to detect or prevent errors and irregularities due to inadequate design and operation, or does not knowingly detect or prevent them;
- residual risk: the risk remaining after management has responded to the risks.

b) Additional risk categories without being exhaustive:

External risks

- Economic
- Legal and regulatory
- Market

Internal risks

- Financial
- Activity
- Human resources

Integrity risks

When considering the above risk categories, integrity risks should be given priority, as integrity risks should be assessed annually in order to ensure that the internal control system is properly implemented in compliance with the law, with proposals for the development of the integrity management system, the responsibility for the assessment and coordination of its implementation resting with the Risk Management Coordinator and the Chancellor.

A suitable methodology for integrity risk assessment could be the methodology developed by the State Audit Office, which would allow the BCE to develop its integrity action plan and its implementation timeframe.

Sectoral guidelines are available for integrity risk assessment, the knowledge and practical application of which is the responsibility of the Risk Management Coordinator, and the action plans developed and issued should be recorded as part of the monitoring system.

The Risk Management Coordinator, in cooperation with the Integrity Advisor, reports on the implementation of the annual integrity-related tasks by 30 September to the Chancellor, who decides on the basis of the report whether to accept or order further action.

Each year the Chancellor is required to issue a statement on the operation of the Internal Control System, which forms part of the budget report.

2. § **Risk analysis**

The set and assessment of risks recorded as part of integrated risk management activities is done by completing a risk management table, where, in addition to quantifiable risks, subjectively assessed risks, risk categories, probabilities of occurrence, and the separation of initial, managed and post-intervention risks are identified. When

assessing risks, we assign three levels of probability of occurrence to the three levels of impact of occurrence on the organisation and objectives.

The response to the risks identified should be decided by determining the level of risk deemed tolerable by the Chancellor, the Vice-Chancellor and the Director of Finance. The risk tolerance is the level of risk exposure above which the organisation will take action in response to the risks it faces.

The person responsible for the analysis and assessment of risks and the definition of the acceptable risk level or tolerance is the number one head of the financial area. The results of the assessment are presented to the Chancellor by the Risk Management Committee, together with recommendations for action, following the periodic review.

The classification of risk levels shall be carried out according to the following table:

Bekövetkezés valószínűsége					
Hatása	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Assessing risks means ranking them in order of significance, based on the likelihood of each risk occurring and the impact they could have on the organisation if they were to occur.

Example of the Risk Assessment Criteria Matrix:		
IMPACT		
Evaluation criteria	**Interpretation**	**Value**
Materiality	The impact of the risk is less than 1% of the annual budget.	1
	The impact of the risk is between 2% and 24% of the annual budget.	2
	The impact of the risk is between 25% and 49% of the annual budget.	3
	The impact of the risk is more than 50% of the annual budget.	4
Vulnerability	A well-regulated and controlled system, with very low risk of irregularities and fraud.	1

	A well-regulated and controlled system where irregularities and fraud are rare.	2
	It is well regulated, but irregularities or fraud can sometimes occur.	3
	Previous audit experience shows a weak control environment, and irregularities and fraud occur.	4
Reputational* sensitivity	No measurable reputational risk.	1
	Reputational damage may occur	3
	It's an area that is exposed to public opinion, so reputational damage can be high.	5
The importance of the process in achieving organisational goals	If it is not working properly, it will only hinder the achievement of your goals.	1
	If it does not work properly, it will have a significant impact on the achievement of objectives, as has been the case in the past in the area concerned.	5
LIKELIHOOD		
Level	**Interpretation**	**Value**
Low	Could happen, but unlikely	1
Medium	Possible in the future	2
High	could happen within 1-2 years	3
Very high	Expected to happen in the near future	4

* Repute or fame

Risks should be assessed according to whether the damage they may cause can be quantified. These parameters are approved by the Chancellor, taking into account the operational characteristics of the Institution.

The formulation of additional assessment criteria for determining impact and likelihood is proposed, to be developed by the Risk Management Coordinator according to the specificities of the organisation and to be promoted in the Committee's work.

3. § **Risk management**

It aims to reduce risks to tolerable levels. Following a risk assessment, an informed decision to take a risk must be made. The decision to mitigate risks means that for each individual risk, it is necessary to ensure that the risk is managed within an integrated risk management plan. When managing risks, given the fact that we have a mandatory core mission in addition to the chosen university activities, it is not always possible to use risk elimination as a management strategy, as in many cases this is not possible, so we must aim to reduce risk exposure by setting a certain tolerance level, which also means that after risk mitigation measures, there remains a certain level of tolerable risk.

Once the risks have been identified and assessed, the Chancellor, depending on his or her competences, decides whether the Institution can take the risk. If the risk cannot be assumed, measures shall be taken to reduce or eliminate it.

The acceptable level of risk is the level above which the Institution will take action or initiate action by the heads of the functions to respond to the risks.

In the framework of an integrated risk management system, risks shall be regularly reassessed on an annual basis, one of the implementation methods being the establishment of a risk management committee with the appointment of the relevant process owners, executives, internal auditor and risk management coordinator. The deadline for completing the annual risk assessment is 30 September each year.

4. § University implementation of integrated risk management

Integrated risk management is not a separate task in the Institution's activities, but is integrated into our daily tasks as part of the internal control system. In the event of changes in the risk environment, new risks must be identified and managed by the persons designated as responsible for this purpose[3], who monitor the operation of the Institution on an ongoing basis and react to changes.

The continuous monitoring of risk management measures as part of the VIR and the monitoring of the status and efficiency of risk management measures across the functions is a permanent responsibility of the heads of the organisational units. If necessary, they shall propose/act to manage the risks, update the regulation of certain activities, if the measures are not having the desired effect, modify them or take new measures.

In view of the above, management should ensure that a near up-to-date system of records is in place to continuously monitor changes in risks and the consequences of management actions. The records shall be submitted with the integrated risk management report, with the tasks for implementation, to the Chancellor, who decides on the further implementation.

5. § The Risk Management Committee

The purpose of setting up the Committee is to implement integrated risk management activities at the University. The members of the Committeeshall be determined annually based on the main processes by the Chancellor, with the agreement of the Rector of the University, with the assistance of the Risk Management Coordinator, who shall ensure the proper conduct of integrated risk management activities by carrying out the following tasks:

a) Preparing the risk assessment along the process map and process descriptions (if no processes are identified and descriptions are not available, they should be prepared, on the basis of which the risk identification should be carried out.) The process map and process descriptions ensure that the risk management system is complete and closed.

b) Grouping and classifying the identified risks.

[3] See Section II/4 of the Regulation.

c) Determining risk factors based on the risks identified.

d) Preparing the risk criteria matrix based on the identified risk factors.

e) Identifying process risks with the assistance of process owners.

f) After examining the elements of the control environment and the measures taken, the Committee sets out the elements for management.

g) Once the risks have been addressed, the value of the modified risk potential is determined.

h) The Committee summarises the analyses and proposals for action and submits them in a report to the Chancellor for approval.

Permanent members of the Risk Committee

The Chancellor shall ensure the implementation of integrated risk management activities at the University at least once a year by establishing a Risk Management Committee and appointing a Risk Management Coordinator to coordinate the activities.

The following aspects should be taken into account when implementing the BCE's integrated risk management activities. The timetable should be such that the risk assessment is completed by 30 September of the year in question at the latest, so that the integrated risk management action plan is completed by 31 October of the year in question, in order to allow internal controls to extract the information it needs to perform its tasks from the risk management system.

6. § **Investigating integrity breaches, in particular fraud and corruption**

Even the best-organised budgetary body may be subject to occasional or recurrent irregularities, due to the negligence or carelessness of staff members or to deliberate breaches of the rules. Given the fact that shortcomings and irregularities jeopardise the achievement of the objectives set by management, it is important that management becomes aware of both intentional and negligent irregularities, if possible, in time to allow for a rapid response and the taking of measures to correct or eliminate the irregularity. Events that breach integrity should be categorised according to whether they are the result of intentional action or negligence. Irregularities shall be dealt with in accordance with the provisions of the rules of procedure for integrity breaches.

Integrity incidents shall always be taken into account in the implementation of the annual risk management tasks, possible risk management methods shall be applied with the help of sectoral guidelines and the proposed measures should be included in the summary report prepared for implementation.

The Chancellor is responsible for the internal regulation of anti-fraud and corruption measures.

IV. Obligation to review the Regulation

The Chancellor is responsible for the preparation and implementation of these rules. The review shall be carried out at least once a year with the assistance of the Risk Management Coordinator.

The proper documentation and implementation of risk management activities is verified by the Director of Finance and the Internal Auditor, who shall report any shortcomings in writing to the Chancellor.

Verification of implementation shall be documented by 10 November each year. The method of verification may include the signature of a report prepared by the Risk Management Committee before submission to the Chancellor.

V. Annexes

1. Model documents for the risk management process
2. Model documents for integrity surveys

Dr. András Lánczi
Rector

Dr. Lívia Pavlik
Chancellor

In witness whereof:

Dr. Marica Sárközi-Kerezsi
Secretary of the Senate