FAKULTA ELEKTROTECHNICKÁ
ZÁPADOČESKÉ UNIVERZITY
V PLZNI

Reference number: ZCU 001433/2020

In Pilsen, on 21 January 2020

# Dean's Directive 1D/2020

# INTERNAL RISK MANAGEMENT SYSTEM

This Directive establishes an internal risk management system for the Faculty of Electrical Engineering (hereinafter referred to as "FEE") at the University of West Bohemia (hereinafter referred to as "UWB") and defines the position and scope of individual components of the internal risk management system. The Directive is based on the principles and best practice established by the RICE Directive, Internal Risk Management System (first edition 2012), which it replaces and extends to cover the entire FEE. Furthermore, this Directive is linked to the risk management of UWB introduced by the Rector's Directive Risk Management System. The basis for the risk assessment is the Strategic Plan of FEE.

## Article 1
## Internal risk management system

(1) The internal risk management system is designed to continuously identify, monitor, evaluate and report significant risks, and has its own organizational structure, effective information support and early warning mechanisms.

(2) The internal risk management system is governed by the following principles:
- total separation from the FEE organizational structure,
- performing independent risk monitoring,
- coordination of risk management with internal audit.

(3) The internal risk management system does not include risks in the area of personal data (GDPR), which are dealt with at UWB level.

(4) Project methodology and risk management are not usually implemented under this Directive. In the case of methodological support, it is possible to contact the risk manager.

(5) The internal risk management system strategy is governed by the principles set out in Annex 2 of the Rector's Risk Management System Directive. The performance of the internal risk management system does not remove the responsibility from executives and project or contract managers for the performance of activities within their competence.

(6) All FEE employees are obliged to contribute to ensuring the functioning of the internal risk management system in accordance with their job title and in accordance with the type of work specified in their employment contract, as specified in their job description.

(7) The FEE Management provides the necessary information, financial, personnel and material resources not only for risk reduction activities, but also for the effective functioning of the internal risk management system.

## Article 2
## Organizational structure of internal risk management system

(1) The organizational structure of the internal risk management system consists of the risk manager and risk owners.

(2) The risk manager:
- provides methodological management and training for risk owners,
- prepares a summary report on risks and submits it to the Dean for approval,
- coordinates activities within the internal risk management system.

(3) The risk manager is appointed by the Dean. The risk manager is directly responsible to the Dean for the performance of his/her duties.

(4) Risk owners:
- are selected FEE employees who are competent to assess the risks in the given area and suggest a method for risk management,
- continuously monitor and evaluate risks in the given area,
- prepare risk owners' reports on the given area of risk management.

(5) Risk owners for each risk area are determined by the Dean following the proposal of the risk manager. The selection of risk owners will take into account their ability to assess risks in the given area and propose an appropriate method of risk management. Risk owners are responsible to the risk manager for their activities.

## Article 3
## Risk management process

(1) The risk management process consists of four successive parts – risk assessment, risk management, risk monitoring and re-examining and the internal risk management system.

(2) Risk assessment is an overall process of risk identification, risk analysis and risk assessment. The risk assessment is based on the methodology set out in Annex 1. The risk owner assesses individual risk areas under the methodological guidance of the risk manager. A record is made by the risk manager in the risk registry set out in Annex 2.

(3) The aim of risk management is to design and implement risk reduction measures. The risk owner will propose measures on the basis of a risk assessment; the Dean or another authorized person decides on the implementation of these measures. Where coordination of measures is necessary, it will be carried out by the designated employee or the risk manager. The risk owner also evaluates whether the residual risk level is tolerable and/or proposes a new measure. The risk management record is made by the risk manager in the risk management plan set out in Annex 3.

(4) Risk owners perform ongoing risk monitoring, check compliance with proposed measures, and communicate with the risk manager on an ongoing basis.

(5) Re-examinations of risks and the internal risk management system should usually be carried out once a year, on 30 June, or as directed by the Dean. On the date of the review, risk owners draw up a report on the risk area entrusted to them, pursuant to Annex 4, and immediately send the report to the risk manager. Based on the reports of individual risk owners, the risk manager prepares a comprehensive report on the risks and the internal risk management system for submission to the Dean for approval.

## Article 4
## Extraordinary risk events

(1) In the event of an extraordinary risk event (incident), the risk owner carries out an impact assessment (e.g. on the operation of the Faculty, financial losses, etc.). In the case of significant consequences or doubts, the risk owner identifies the source of the incident and suggests operational measures, which he/she immediately convey to the risk manager, see the Incident report in Annex 5.

(2) The risk manager assesses the proposed measures according to their level and impact, and informs the Dean of this incident. The Dean operatively decides, depending on the severity of the incident, on any further steps.

(3) An incident is considered closed if the effectiveness of the implemented operational measures is sufficient or evaluated as insignificant for the operation of the Faculty. The Dean informs the risk manager and the risk owner about the closure of the incident.

**Article 5**
**Transitional and final provisions**

(1) This Directive enters into force on the day of its signature.

(2) This Directive replaces the directive RICE-S-02-2017 Internal Risk Management System applicable to RICE. The last review under the RICE directive takes place in June 2020.

(3) The first risk assessment under this Directive will be carried out on 30 September 2020 at the latest.

(4) The first review of the risk management system under this Directive will take place on 30 June 2021.

(5) Risk management processes are graphically illustrated at https://fel.zcu.cz/procesy/.

(6) Annexes to the Directive:
- Annex 1 – Risk management methodology
- Annex 2 – Risk registry
- Annex 3 – Risk management plan
- Annex 4 – Risk owner's report
- Annex 5 – Incident report

Prof. Ing. Zdeněk Peroutka, Ph.D.

Dean of the Faculty of Electrical Engineering of the University of West Bohemia

# RISK ASSESSMENT METHODOLOGY

The risk assessment methodology includes risk identification, risk analysis and risk assessment.

The proposed risk analysis is a combination of qualitative and quantitative risk analyses. This methodology is applicable to risk analysis of processes (activities) or defined assets (objects/buildings). Its principle is to define a system (an object/a building) or process that will be subject to risk analysis. This object represents FEE's assets, which can be expressed in financial terms based on own valuation or data taken from the accounting.

If objects are defined, then activities (processes) that can create a risk can be defined relative to these objects. Thus, one or more risks can be identified for each process, and the risk rate can be expressed using a defined risk factor.

The risks are recorded in the **risk registry** – using the following structure:

- Risk Code – a code designation of the risk that is used to identify and refer to the risk as required,
- Activity (process) – a description of the actual activity that is performed on a defined object, or assets (of the object),
- Risk – identification of a danger (source of risk) – written description of the risk or source of risk,
- Risk assessment – is part of the whole risk evaluation and determines the risk rate. Risk assessment consists of three factors:
    - consequence (N),
    - probability (Pst) and
    - risk factor (RF).
- Current measures – measures (activities) that have been carried out (done) and whose outcome affects the risk assessment,
- Current management method – current risk management method: activities that are currently taking place (carried out), are not completed, or could be increased in intensity if the risk arises,
- Risk Management Yes/No – information as to whether the risk will be included in the Risk Management Plan.

**Consequence (N)** expresses numerically the "strength" of the risk according to its consequences (see the following table). The severity of the risk is the square of the risk rate.

| Risk rate | Consequence | Characteristics | Description of the risk severity – typical attributes |
|---|---|---|---|
| 1 | 2 | Insignificant | Insignificant breach of workflow within an organization with immediate remediation possibility with zero financial loss. |
| 2 | 4 | Small | Minimum financial loss, interruption of work for less than eight (8) hours with immediate remediation possibility. |
| 3 | 8 | Medium | Financial losses of up to 5% of the contract price of a contract or a project for an order, interruption of work for less than 24 hours and additional costs for putting laboratories into operation, breach of legislative obligations, safety at work, sanctions, fines and penalties, ineligible costs below 10,000 CZK. |
| 4 | 16 | Large | Interruption of work from 2 to 30 business days, financial losses from 10% to 50% of the total amount of the |

| | | | |
|---|---|---|---|
| | | | planned order (project) revenue, damage to reputation, customer loss by 25%, sanctions, fines and penalties, ineligible costs over 10,000 CZK. |
| 5 | 32 | Catastrophical | Unplanned interruption of work for more than 30 days, enormous financial losses over 50% of the total planned order revenue, customer loss by 50%, sanctions, fines and penalties, ineligible costs over 100,000 CZK, non-compliance with binding monitoring indicators. |

**Probability (Pst)** is the probability of occurrence of a risk and is based primarily on practical experience depending on the probability of the given risk occurring. Each probability grade is assigned a severity that is recorded in the risk analysis table. The probability of a risk can be expressed as defined in the following categories:

| **Pst** | **Description of the probability of risk occurrence** |
|---|---|
| 1 | An almost impossible occurrence |
| 5 | Not common, but may occur under special circumstances |
| 10 | Possible occurrence |
| 15 | Frequent occurrence |
| 20 | Extremely frequent, repetitive occurrence |

**Risk factor (RF)** is the resulting rate of risk, determined by a calculation, namely multiplication of the consequence (N) by the probability (Pst). Based on the risk factor, it is possible to identify the **risk group** as a result of the full risk assessment. The size of risk factor is decisive for deciding whether or not the risk should be managed. The risk group is determined by the size of the risk factor:

| **Risk group** | **Risk factor** | **Description** | **Risk Management Plan** |
|---|---|---|---|
| 1 | bellow 20 | common risk; compliance with common standards and procedures in this area is recommended. | No |
| 2 | 21-240 | increased risk level; continuous risk monitoring and possible introduction of operational technical or organizational measures are recommended. | No |
| 3 | over 241 | very high level of risk; it is recommended to take technical and organizational measures to eliminate the risks. | Yeas |

**Risk Management Plan** contains a list of proposed and implemented risk measures for the highest risk group – 3 – using the following structure:

- Risk code – code identification of the risk from the risk registry,
- Proposed measure – designation of a group of risk reduction measures,
- Proposed method of implementation (description) – specification of activity in the group of measures,
- Responsible person – the nominated person or the person responsible for implementation,
- Implementation date – the proposed date of implementation,
- Financial requirements – an estimate of the financial costs (if necessary),
- Approved for implementation Yes/No – the result of the Dean's decision to implement the proposed measure,
- Actual date of implementation – in the case of implementation, the actual implementation date is given; it usually corresponds to the proposed implementation date.

FAKULTA ELEKTROTECHNICKÁ
ZÁPADOČESKÉ UNIVERZITY
V PLZNI

# Registr rizik / Risk register

Datum zpracování / date of processing:

| **Kód rizika** Risk code | **Činnost (proces)** Activity (process) | **Riziko - identifikace nebezpečí (zdroj rizika)** Risk - hazard identification (risk source) | **Ohodnocení rizika** Risk evaluation | | | **Současná opatření** Current control | **Současný způsob řízení** Current management | **Ošetření rizika Ano/Ne** Risk treatment yes / no |
|---|---|---|---|---|---|---|---|---|
| | | | **N** | **Pst** | **RF** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |
| | | | | | **0** | | | |

FAKULTA ELEKTROTECHNICKÁ
ZÁPADOČESKÉ UNIVERZITY
V PLZNI

# Plán ošetření rizik / risk treatment plan

Datum zpracování / date of processing:

| **Kód rizika**<br>Risk code | **Navržené opatření**<br>Proposed countermeasure | **Navrhovaný způsob realizace (popis)**<br>Suggested implementation (description) | **Odpovědná osoba**<br>Responsible person | **Termín realizace**<br>Date of implementation | **Finanční požadavky**<br>Financial requirements | **Schváleno k realizaci Ano/Ne**<br>Approved for implementation Yes/No | **Skutečný termín realizace**<br>Real date of implementation |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

FAKULTA ELEKTROTECHNICKÁ
ZÁPADOČESKÉ UNIVERZITY
V PLZNI

# ZPRÁVA VLASTNÍKA RIZIK

**Risk owner report**

Oblast rizik:
Risk area .....

Vlastník rizik:
Risk owner .....

Datum posouzení rizik:
Date of risk evaluation .....

Podpis vlastníka rizik:
Signature of risk owner: .....

| Informace o plnění navržených opatření za minulé období<br>Information on implementation of the proposed countermeasures in the previous period |
|---|
| |

| Výsledky posouzení rizik<br>Results of risk evaluation |
|---|
| |

| Navržený plán ošetření rizik<br>Proposed plan for risk treatment |
|---|
| |

| Vzniklé rizikové události (incidentu) ve sledovaném období (příčina, následky, opatření)<br>Risk event occured in reporting period (cause, consequence, control) |
|---|
| |

| Poznámky a návrhy ke zlepšení interního systému řízení rizik<br>Comments and suggestions to improve the internal risk management system |
|---|
| |

FAKULTA ELEKTROTECHNICKÁ
ZÁPADOČESKÉ UNIVERZITY
V PLZNI

# HLÁŠENÍ UDÁLOSTI (INCIDENTU)

**Risk event report**

Oblast rizik:
Risk area .....

Vlastník rizik:
Risk owner .....

Popis události:
Event description .....

Datum vzniku události
Date of event start .....

Příčina události:
Event cause .....

Vyhodnocení dopadů:
Impact assessment .....

Navržená nápravná opatření:
Proposed countermeasures .....

Datum a čas hlášení:
Date and time of report .....

Podpis vlastníka rizik:
Risk owner signature .....

## Stanovisko manažera rizik

**Statement of the risk manager**

Datum převzetí hlášení:
Date of report evidence .....

Datum stanoviska:
Date of statement .....

Podpis manažera rizik:
Risk manager signature .....

## Rozhodnutí děkana o řešení události (incidentu) a realizaci nápravných opatření

**Dean's decision about event treatment and countermeasures**

Datum převzetí hlášení:
Date of report evidence .....

Datum uzavření události:
Date of event closing .....

Podpis děkana:
Dean signature .....