EUROPEAN
UNIVERSITY
INSTITUTE

Risk Management Framework

Office of the Secretary General

RM-V1/R0 (October 2021)

Table of Contents

Introduction

This document outlines the European University Institute’s (EUI) Risk Management Framework. It is structured in three sections: The Risk Management Policy, outlining the guiding principles; the Risk Management Process, outlining the practical implementation of Risk Management; and corresponding annexes.

This framework formalises a structured approach to managing risk across all units of the EUI, both administrative and academic, as part of the Internal Control Framework. It aims to assist the organisation in integrating risk management into its strategic planning, annual reporting, and the budgetary cycle. In addition, the framework seeks to foster a culture of risk management across the planning, monitoring and reporting of EUI’s activities at all levels.

The overarching responsibility for risk management lies with the Secretary General in his/her capacity of Chief Risk Officer, who is also the owner of horizontal risks. Risk owners in each unit are responsible for identifying and managing unit-level risks, supported by risk management contact points delegated by each unit.

While the effectiveness of risk management will depend on its successful integration into governance practices, including decision-making, it will also depend on recognition by risk owners across all units as a common endeavour. More generally, all members of the EUI community should consider the risks involved in the activities they carry out for the EUI.

The Risk Management Framework is owned by the Office of the Secretary General and is aligned with best practices in risk management in order to ensure the achievement of the EUI’s strategic, general and specific objectives.

This framework is designed based on the principles of ISO 31000 "Risk management -- Principles and guidelines".

1.1. Key terms and definitions

1.1.1. Existing controls: Controls that are already in place, i.e. have been implemented in the past.
1.1.2. Event: An occurrence or change in a particular set of circumstances.
1.1.3. Impact: The nature and magnitude of the consequences of a risk manifesting.
1.1.4. Hazard: Something with the potential to cause harm.
1.1.5. Inherent risk: Risk assessment (impact x likelihood) without any controls in place.
1.1.6. Likelihood: The chance of the risk occurring.
1.1.7. Opportunity: An outcome of a risk that is positive for the organisation.
1.1.8. Residual risk: The risk rating after considering the effectiveness of the internal controls designed to manage the risk.
1.1.9. Risk: The effect of uncertainty on objectives.
1.1.10. Risk assessment: Calculation of impact rating times likelihood rating (see annex 2, point c, for risk assessment calculation).
1.1.11. Risk No: Code assigned to the risk for easy identification, monitoring and tracking in the CRR.
1.1.12. Risk owner: Directors of Service and Heads of Academic Units responsible for the risk.
1.1.13. Risk Management: Coordinated activities and common guidelines to direct and control the effects of risk on the EUI and its objectives.
1.1.14. Risk Management Framework: A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organization.
1.1.15. Risk Management Process: The systematic application of management policies, procedures and practices to the tasks of communication, consultation, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.
1.1.16. Risk response: Risk owner’s decision to accept the risk or act upon the risk by introducing further controls.
1.1.17. Uncertainty: The state of not knowing how or if potential events may manifest.

2. EUI Risk Management Policy

2.1. What is a risk?

Risk is the possibility that events will occur and affect the achievement of strategy and business objectives. ISO 31000 defines risk as "The effect of uncertainty on objectives".

A risk begins with a problem/hazard/issue/uncertainty (factor) that could cause damage to a person or the institution and its activities. A risk assessment will begin with a mapping of these factors, which will only then be considered a risk if it has an impact on the achievement of an institution's objectives. If not, it remains simply a problem/hazard/issue/uncertainty with relevant preventative measures in place. Therefore, a risk is the chance that the institution will be harmed by a factor, with a negative effect the achievement of its objectives, if it were to manifest.

2.2.What is Risk Management?

Risk management is a broadly recognised management concept that is applied both in public organisations and in the private sector to identify and manage obstacles or incidents that could hinder the achievement of an organisation's objectives or the execution of its key activities. In addition, risk management focuses not only on the negative, but also exploits the positive outcomes of risks, known as opportunity, and manages them in such a way that stimulates the organisation's development.

Good risk management goes beyond the immediately identified risks. It carries out an issues-analysis in the annual reporting phase of internal control, which digs deeper to reveal previously unidentified risks that affected the achievement of objectives over the reporting year. Such analysis consequently informs adjustments to the Risk Management Framework, leading to its optimisation for the future.

2.3. Scope of Risk Management

The EUI focuses on risks in the following categories:

- Strategic: Risks relating to the effective alignment of the EUI's long-term strategic direction, its strategy, mission and vision, the needs of its contracting states, and the organisation's role in achieving the goals of the Convention.
- Governance: Risks relating to the involvement of stakeholders at all levels.
- Operational: Risks relating to the effectiveness and efficiency of internal processes.
- Financial: Risks relating to adequacies in financial resources and their management.
- Compliance: Risks relating to compliance with the provisions of the EUI Convention, EUI Financial Rules and internal procedures.

At the same time, reputational risk is an integral element in managing the above categories of risks. Risk owners always need to assess potential risks to the reputation of EUI when determining how to manage their risks.

2.4. Benefits of Risk Management

The benefits of establishing a Risk Management Framework include, but are not limited to:

- ✓ Greater assurance that the objectives at all levels (priorities of the EUI strategy, plus the general and specific objectives) will be met.
- ✓ Better internal controls, accountability and business continuity.
- ✓ Improved ability to anticipate change and increase organisational agility.
- ✓ Improved stakeholder confidence and trust.
- ✓ Better assurance that assets are safeguarded.
- ✓ Protected institutional reputation.
- ✓ Better resources management.
- ✓ Improved organisational resilience in the face of change.
- ✓ Improved organisational learning.
- ✓ Identification of unanticipated opportunities that benefit the organisation's development.

2.5. Approach to Risk Management

The EUI adopts the following cyclical approach to its Risk Management:

Plan: The EUI has an institutional strategy and identifies related general and specific objectives. In view of ensuring the achievement of its strategic priorities and objectives, the EUI has recognised the need for integrated approach to managing risks and for the establishment of an institutional Risk Management Framework. It has devised a risk management process to respond effectively and efficiently to risk. It has a Chief Risk Officer (CRO) and nominates risk owners and contact points responsible for monitoring risks within its units.

Do: The EUI Secretary General coordinates an institution-wide Risk Management Exercise in which all units submit their risks to a Central Risk Register (CRR), maintained by the Office of the Secretary General. Unit-level risk owners identify, analyse, monitor and evaluate risks relating to their specific objectives that are submitted to the CRR. The Secretary General (as CRO) identifies, analyses, monitors and evaluates horizontal objectives, and identifies horizontal risks with input from the Management Team. The EUI trains personnel involved in risk management across the institution.

Check: The EUI carries out an issues-analysis during the reporting phase. Risk owners evaluate whether objectives not met were hampered by risks present in the CRR or unidentified risks. This analysis checks the effectiveness of the Risk Management Framework.

Act: Risk Management performance is reviewed and reported to draw on lessons learnt. The Risk Policy and Process are adjusted accordingly to reflect these lessons. Necessary new training is provided.

2.6. EUI Principles for Risk Management

Risk management at the EUI is guided by the following principles:

2.6.1. It is integrated into planning, reporting and internal control: Risk management is not a stand-alone activity that is separate from the main activities and processes of the organisation. It is part of management's responsibilities and an integral part of relevant business processes at all levels, from strategic direction to project planning.

2.6.2. It is a structured, systematic, and comprehensive exercise: Approaching risk management according to a structured and comprehensive framework with a systematic approach facilitated with guidelines contributes to consistent and comparable results.

2.6.3. Staff at all levels take ownership: Risk owners at all levels are conversant with all types of risks (including those the EUI's reputation) affecting their unit-level objectives. They use appropriate processes to assess, monitor and mitigate the risks they identify.

2.6.4. It is dynamic: Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

2.6.5. It uses best available information: Input to risk management is based on historical and current information, as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

2.6.6. It considers human and cultural factors: Human behaviour and culture significantly influence all aspects of risk management at each level and phase.

2.6.7. It is continually improved: The Policy and Process for managing risk at the EUI are analysed annually, drawing lessons learnt that inform the framework's optimisation.

2.7. Horizontal Risks

Based on an annual analysis of the CRR, the Chief Risk Officer identifies and manages a set of horizontal risks, which:

- Have a far-reaching and widespread impact on the achievement of the strategic priorities and general objectives.
- Have a potentially detrimental effect on the overall functioning and existence of the EUI.
- Involve more than two EUI units.
- Have a risk assessment of more than 16.

Horizontal risks are discussed within the Management Team.

The presence of a horizontal risk does not eliminate a risk of the same nature at unit level.

2.8. Risk Management Tools

2.8.1. Central Risk Register

All EUI risks are recorded as an inventory in the Central Risk Register (CRR), managed by the Office of the Secretary General. Risks are submitted to the CRR once a year during the planning phase. The CRR contains a dedicated column to connect the risks recorded in the CRR to strategic, general and specific objectives. Each risk is coded with a risk number.

Each unit keeps updated the part of the CRR that is relevant to their activities.

For the CRR format, see annex 1.

2.8.2. Submission template

Unit-level risks are submitted to the CRR using the dedicated template in Excel. Risks cannot be submitted to the CRR in any other form.

2.8.3. Objective inventory

The objectives inventory accompanies the CRR. It contains coded objectives, which are used to indicate the associated objectives for each risk on the CRR.

2.9. Timing and Frequency

At corporate level, risks are submitted annually to the CRR during the planning phase. Risks are monitored regularly throughout the year at the discretion of the risk owner and reported on in the corporate reporting phase. The CRO may request an additional corporate risk assessment at any given moment.

At unit level, risks are managed on a continuous basis at least once a month.

2.9.1. Corporate planning

Risks are assessed during the planning phase in the framework of objective-setting. For every objective set, the associated risks are identified. Risks identified during planning are submitted to the CRR and analysed by the Chief Risk Officer, who then identifies horizontal risks.

2.9.2. Monitoring

Risk owners carry out regular monitoring (ideally at least once a month) of their risks and ensure that the planned actions are being implemented. Risk owners communicate any significant changes in their risks to the Chief Risk Officer as soon as the change is identified.

2.9.3. Corporate reporting

The assessment of the risk management process, including the effectiveness of mitigating actions towards risk in the achievement of objectives, takes place during the annual reporting phase. It includes analysis of issues that affected the timely achievement of objectives.

2.10. Accountability and Responsibility for Managing Risk

2.10.1. Institutional responsibility

EUI President: The EUI President carries out a final review of the CRR at the end of the corporate planning phase. He/she also reviews the units' Annual Activity Reports at the end of the reporting phase, in which an assessment of the risk management process is integrated.

Chief Risk Officer: The Secretary General is the Chief Risk Officer (CRO) and has executive responsibility for the EUI's risk management. He/she demonstrates and articulates his/her continual commitment to risk management through the present Framework.

The CRO is responsible for:

a. Reviewing and monitoring the Risk Management Framework.
b. Monitoring its implementation and compliance.
c. Providing advice to risk owners with a view to controlling the quality of risk management, especially on risk rating.
d. Maintaining an institutional Risk Register, containing risks from all units.
e. Analysing results from planning and reporting processes, and incorporating findings as required into the CRR and into the Risk Management Framework.
f. Ensuring the Risk Management Framework interacts with other key organisational processes.
g. Identifying horizontal risks, defining risk ownership, mitigating actions and monitoring their implementation.
h. Keeping risk owners, via Management Team Meetings, updated on adjustments to the Risk Management Framework and of lessons learned during the exercise.

2.10.2. Strategic responsibility

The **Management Team** is the primary management forum for discussing the EUI's approach to risk management and for providing guidance on risk management, as required, including, but not limited to a list of risks and risk treatment. It has an opportunity to discuss (new) risks, share feedback on the Risk Management Framework and its implementation. In principle, the Management Team makes Risk Management a regular point on the agenda of its meetings.

2.10.3. Unit-level responsibility

Risk Owner: Directors of Service and Heads of Academic Units are risk owners. They are accountable for the risks in their units and have the authority to manage (identifying, assessing and treating) risk in the area under his/her responsibility, in accordance with the Risk Management Framework. Risk owners apply the Risk Management Framework to the formulation of their Action Plans when objective-setting for the unit and in resource allocation and establishment of key performance indicators.

Risk Management Contact Points in each unit may be nominated by the risk owners to facilitate work at unit level. Contact points assist risk owners in the implementation of risk management in their unit, in particular but not limited to, reviewing and updating risk registers and maintaining communication with the CRO. Each nomination is communicated to the CRO.

2.10.4. Guidance on risk management

The IAO provides guidance and advice to the EUI President and CRO on coordinating risk management at institutional level, as well as to risk owners in the operational management of risks in their units. The role of the Internal Audit Office (IAO) is defined in Article 60 of the EUI Financial Rules and the IAO Charter.

2.10.5. Common responsibility

All members and all non-members carrying out activities at the EUI are responsible for managing risks related to their areas of operation even if it is not in a formal capacity. They assist risk owners in their risk management in accordance with this Risk Management Framework by maintaining an awareness of risk within the activities they carry out. Risks can be identified by any person carrying out activities for the EUI and are reported to the risk owner or delegated contact point in the relevant unit.

2.11. Training, Reviewing and Optimising

The present Framework is reviewed by the Office of the Secretary General at least every three years during the reporting phase, when any opportunity for optimisation is implemented.

Any individual holding a role and responsibilities as outlined above receives formal trainings on risk management. Training is organised and delivered by the Office of the Secretary General and the Internal Audit Office, with support from the Human Resources Service, at least every three years and on the occasion of any significant amendments to the Framework.

2.12. Communication and Consultation

Throughout the risk management process, risk owners ensure timely communication and consultation with all relevant stakeholders, including those in other units. The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making.

2.13. Entry into force

This Framework is effective from 6 October 2021.

3. Risk Management Process

Risk management is a continuous exercise that spans the entire EUI planning and reporting cycle, beginning with objectives-setting.

Corporate planning phase

3.1. Risk assessment of objectives

Unit level

Identify your risks: When setting objectives, consider what factors may affect the achievement of those objectives (whether strategic priorities of the strategy, general or specific objectives), and thus identify the risks associated to those objectives, i.e. a risk is when there is a chance the objective will not be achieved should a factor cause harm to the organisation.

Analyse your risks: Complete the CRR template with new risks and update existing risks identified. This template is also used as the unit-level risk register.

- Describe the risk (how and why it affects the objective);
- Calculate the inherent risk: What is the likelihood of the risk occurring and its impact on the objective if no controls are in place? See annex 2 for the risk rating guidelines.
- Indicate the existing controls: What controls are already in place that mitigate this risk?
- Calculate the residual risk: What is the likelihood of the risk occurring and its impact on the objective with the existing controls in place? See annex 2 for the risk rating guidelines.

- **Evaluate your risks:** Decide how you will respond to the risk (*Accept* or *Act*): Is this risk acceptable as it is based on the EUI's level of risk appetite or can further action be taken to mitigate it? If Accept, justify why no further actions can/should be planned.

3.2. Risk Treatment

If Act, plan how you will treat your risk: Identify and select planned actions: What else can be done to further mitigate the risk?

- Select other controls that you plan to put in place in the future to reduce the risk.
- Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits of running the risk vis-à-vis the achievement of the objectives against the cost, efforts, or disadvantages of implementation.

3.3. Submission to the Central Risk Register

Submit your risks to the CRR: Send your template completed with your unit's risks to the Office of the Secretary General.

3.4. Analysis of the Central Risk Register

Coordination level

Evaluation of the CRR: The Office of the Secretary General inserts new risks into the CRR and updates previously identified risks. The CRO analyses the CRR, requesting clarifications from risk owners where necessary.

Identification of horizontal risks: With input from the Management Team, the CRO identifies horizontal risks. The CRO analyses and evaluates the horizontal risks and determines their treatment with the same methods as outlined for the unit level.

The CRR is submitted to the EUI President.

Monitoring phase

3.5. Systematic monitoring of risks

Unit level

Monitor your risks regularly: Use the unit-level risk register to check for any changes to your risks regularly and systematically and ensure that the controls are being implemented. A good habit is to check your risks at least every month.

Report significant changes: If you notice any significant changes to your risk ratings or the risk in general, communicate it immediately to the CRO.

Coordination level

Monitor horizontal risks regularly: The Office of the Secretary checks for any changes to the horizontal risks and ensures the controls are being implemented.

Regular Risk Management reviewing: The Management Team holds regular discussions on the management of the organisation's risks during its monthly meetings. In addition, the July session of the Management Team Meeting is dedicated to a mid-term review of objectives and their related risks.

Reporting phase

3.6. Risk Assessments in Activity Reports

Unit level

Include an assessment of the Risk Management Process in your Activity Report: Assess the effectiveness of planned mitigating actions towards risks in the achievement of objectives.

- Controls evaluation: Were your controls (existing controls and planned actions) effective in mitigating the risk? If not, why not and consider how they can be improved.
- Carry out an issues-analysis: Was the achievement of your objectives affected by risks present in the CRR or by other unidentified risks?
- Process evaluation: how effective is the Risk Management Process in your unit? Is the risk assessment exercise helpful in achieving objectives?

Coordination level

Secretary General's Activity Report: The Secretary General includes an assessment of the Risk Management Process in his/her annual activity report. The assessment includes, as above, an evaluation of the controls and an issues-analysis.

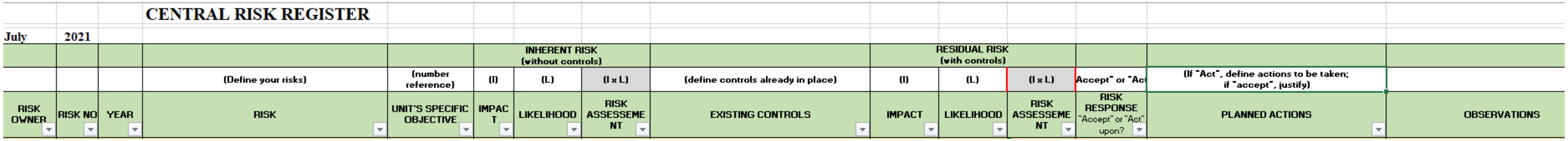
3.7. Optimisation of the Risk Management Framework

Coordination level

Lessons learnt: Based on emerging areas of weakness in the Risk Management Framework, the Office of the Secretary General, with input from the Internal Audit Office and the Management Team, identify and implement improvements to the Framework.

Training: If there are significant revisions to the Risk Management Framework, staff are provided relevant training before the next planning phase.

Annex 1 | EUI Central Risk Register format



			CENTRAL RISK REGISTER											
July	**2021**													
					INHERENT RISK (without controls)				RESIDUAL RISK (with controls)					
			(Define your risks)	(number reference)	(I)	(L)	(I x L)	(define controls already in place)	(I)	(L)	(I x L)	Accept" or "Act	(If "Act", define actions to be taken; if "accept", justify)	
RISK OWNER	RISK NO	YEAR	RISK	UNIT'S SPECIFIC OBJECTIVE	IMPACT	LIKELIHOOD	RISK ASSESSMENT	EXISTING CONTROLS	IMPACT	LIKELIHOOD	RISK ASSESSMENT	RISK RESPONSE "Accept" or "Act" upon?	PLANNED ACTIONS	OBSERVATIONS

- ➢ **Risk owner:** Head of Unit responsible for the risk.
- ➢ **Risk No:** Code assigned to the risk for easy identification, monitoring and tracking in the CRR.
- ➢ **Related objective:** Number of the objective to which the risk relates (taken from objective inventory).
- ➢ **Inherent risk:** Risk assessment (impact x likelihood) without any controls in place.
- ➢ **Existing controls:** Controls that are already in place, i.e. have been implemented in the past.
- ➢ **Residual risk:** Risk assessment (impact x likelihood) with existing controls in place.
- ➢ **Impact:** Rating assigned for the impact of risk on the achievement of objectives (see annex 2, point a, for rating calculation).
- ➢ **Likelihood:** Rating assigned for the likelihood that the risk identified will materialize (see annex 2, point b, for rating calculation).
- ➢ **Risk assessment:** Calculation of impact rating times likelihood rating (see annex 2, point c, for risk assessment calculation).
- ➢ **Risk response:** Risk owner's decision to accept the risk or act upon the risk by introducing further controls.
- ➢ **Planned actions:** Further actions (controls) selected to implement to mitigate the risk, i.e. additional controls that will be implemented in the future.
- ➢ **Observations:** Comments made by the CRO or risk owner (optional)

Annex 2 | Calculating the risk rating

The total risk rating is the likelihood rating multiplied by the impact rating.

a. Likelihood rating

Rating	Description
1	Highly unlikely, but it may occur in exceptional circumstances. It could happen but probably never will (10% or less Probability).
2	Not expected, but there's a slight possibility it may occur at some time (10-35% Probability).
3	The event might occur at some time, notably if there is a history of occasional occurrence at the EUI (35-65% Probability)
4	There is a strong possibility that the event will occur, notably if there is a history of frequent occurrence at the EUI (65-90% Probability).
5	The event is expected to occur in most circumstances, notably if there is a history of regular occurrence at the EUI (90% or greater Probability).

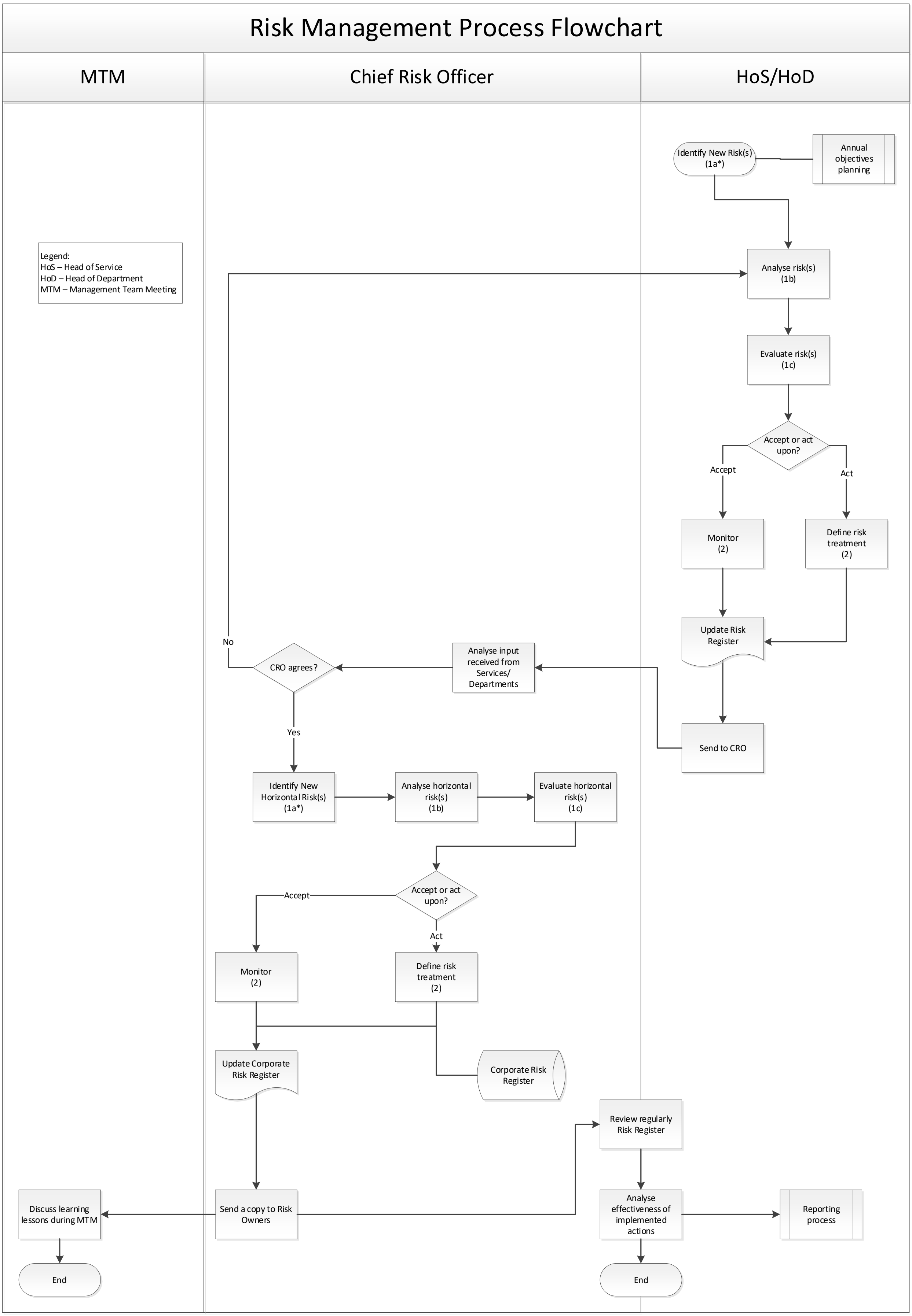
b. Impact rating

Rating	Description
1	If the risk occurs, it will have no impact on the EUI or the delivery of desired results, in that the core and/or programme objectives will be achieved.
2	If the risk occurs, it will have a minor impact on the EUI and/or the delivery of desired results, in that the achievement of one or more core and/or programme objectives may be delayed.
3	If the risk occurs, it will have a moderate impact on the EUI and/or the delivery of desired results, in that one or more core and/or programme objectives may only be partially achieved.
4	If the risk occurs, it will have a significant impact on the EUI and/or the delivery of desired results, in that one or more core and/or programme objectives will likely not be achieved.
5	If the risk occurs, it will have a significant impact on the EUI and/or the delivery of desired results, in that one or more core and/or programme objectives will not be achieved.

c. Risk matrix

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	1	5
Likelihood / Impact	1	2	3	4	5

Annex 3 | Risk Management Process Flowchart


Risk Management Process Flowchart
MTM
Chief Risk Officer
HoS/HoD
Legend:
HoS – Head of Service
HoD – Head of Department
MTM – Management Team Meeting
Identify New Risk(s) (1a*)
Annual objectives planning
Analyse risk(s) (1b)
Evaluate risk(s) (1c)
Accept or act upon?
Accept
Act
Monitor (2)
Define risk treatment (2)
Update Risk Register
Send to CRO
Analyse input received from Services/ Departments
CRO agrees?
No
Yes
Identify New Horizontal Risk(s) (1a*)
Analyse horizontal risk(s) (1b)
Evaluate horizontal risk(s) (1c)
Accept or act upon?
Accept
Act
Monitor (2)
Define risk treatment (2)
Update Corporate Risk Register
Corporate Risk Register
Review regularly Risk Register
Send a copy to Risk Owners
Discuss learning lessons during MTM
Analyse effectiveness of implemented actions
Reporting process
End
End

*Numbers in brackets correspond to the section of the Risk Management Process description included in Annex 1