


# Enterprise Risk Management Policy

# Contents


**1. Introduction ..... 1**

1.1 Overview of Enterprise Risk Management ..... 1

1.2 Purpose of UL Enterprise Risk Management Policy ..... 1

1.3 Scope ..... 2

1.4 Definitions ..... 3

**2. Policy Statement ..... 4**

**3. Context ..... 4**

3.1 Legal and Regulatory Context ..... 4

3.2 Other Context ..... 5

**4. How the Risk Management Framework Works ..... 5**

4.1 Risk Management Process Overview ..... 5

4.2 Five Core Stages ..... 6

4.3 Tools and Systems ..... 12

4.4 Practical Workflow Example: From Risk Identification to Closure ..... 12

4.5 Key Success Factors ..... 14

**5. Related Procedures for Enterprise Risk Management ..... 15**

5.1 Overview of Risk Management at UL ..... 15

5.2 Roles and Responsibilities ..... 16

5.3 Categorising Risk ..... 18

5.4 Risk Appetite ..... 19

5.5 Risk Management Cycle ..... 20

5.6 Managing Risk ..... 22

5.7 Risk Management Model ..... 22

**6. Related Documents ..... 24**

**7. Document Control ..... 24**

# 1. Introduction

## 1.1 Overview of Enterprise Risk Management

University of Limerick (UL) applies a structured, integrated and consistent approach to identifying, assessing and managing risks and opportunities that may affect the achievement of its academic, research, operational and strategic objectives. Risk management informs decision-making, planning and performance management and supports the University in operating within its approved risk appetite.

UL is committed to ensuring that risk management is seen as everybody's responsibility, is part of regular day-to-day business, and informs both the strategic and operational planning and performance cycle. Enterprise risk management is underpinned by a comprehensive framework for making risk-based decisions that support achieving our strategic goals. Currently, UL's goals focus on education, research, internationalisation and supporting our broader community in the mid-west region. As we develop and revise our strategic plan, these goals and risk emphases may change. While all staff contribute by identifying and escalating risks within their remit, accountability for managing each risk rests with designated risk owners, with escalation to the appropriate governance level where risk exceeds appetite, tolerance or delegated authority. Enterprise risk management supports coherent management of risks and opportunities across the University, avoiding fragmented or inconsistent responses.

## 1.2 Purpose of UL Enterprise Risk Management Policy

The purpose of this policy is to establish the principles, governance and minimum requirements for identifying, assessing, measuring, monitoring, reporting and managing risks and opportunities that arise within the University, and to ensure that risk information supports decisions and provides assurance that the University is operating within its approved risk The policy forms one component of the UL Risk Management Framework.

**The policy is designed to**

- help UL staff to understand their role and the need to adopt a consistent approach to the assessment and management of risk
- set out the systems and processes required to ensure that risks are managed consistently across the University
- establish minimum standards for risk assessment, recording, review and reporting across all units;
- contribute to bringing about a culture where open communication is encouraged to identify and mitigate potential risks before they occur

**This policy supports this purpose by**

1. establishing a framework to identify, assess and treat risks through controls and time-bound actions;
2. supporting reasonable assurance through clear ownership, documented controls, monitoring, reporting and independent assurance activities;
3. requiring that residual risks are evaluated against the Risk Appetite Statement and escalated where thresholds or delegated authority limits are exceeded.

Effective risk management involves identifying, assessing and treating l risks (avoid, reduce, transfer or accept), which helps us identify and capitalise on opportunities. This approach enables us to

proactively manage uncertainties while maximising the potential for success in all fields of our activities – academic, administrative and support.

Some of the benefits associated with effective risk management include

- being more resilient in the face of threats to achieving what matters to UL and its staff
- being better able to achieve and demonstrate good corporate governance
- complying more fully with legal and regulatory requirements
- having transparent processes and examples of good practice
- having risk-aware staff and a risk-aware culture
- being better able to support management decisions
- being able to respond to emerging and evolving risks swiftly and in a structured manner
- improving public accountability and transparency
- improving the quality and efficiency of processes
- being able to prioritise immediate risk
- instilling a positive attitude to implementing risk controls

## 1.3 Scope

### 1.3.1 To whom does this policy apply?

This policy applies to all members of the UL community and to all subsidiary companies. Subsidiaries adopt the same principles and may either adopt this policy directly or implement an equivalent policy aligned with UL's framework. For consistency and oversight, subsidiaries use the University's Risk Management Information System (RMIS) to maintain risk registers and reports.

### 1.3.2 In what situations does this policy apply?

This policy applies to matters relating to operations and activities over which UL has ownership, control or legal responsibility. The policy does not apply to personal matters unrelated to UL's operations nor to external activities where UL has no ownership, control or legal responsibility. For example, personal consultancy work undertaken by staff entirely in a private capacity, unrelated to their role at UL, falls outside the scope of this policy[1].

Additionally, this policy does not override specific legal, regulatory, or contractual risk management obligations (e.g., research projects funded by external agencies, such as the European Union, may be subject to mandatory risk management processes defined in the funding contract). Similarly, compliance with statutory health and safety obligations under Irish law is governed by specific legislative requirements. However, where such activities create risks that could materially affect UL's objectives, operations, finances, compliance or reputation, those risks must be recorded, monitored and escalated through UL's ERM framework.

[1] Personal consultancy undertaken **entirely in a private capacity** (i.e., not part of UL duties and not presented as UL-endorsed) falls outside this policy. However, where consultancy could **create risks for UL**, for example, if an individual is, or could be perceived as, acting on behalf of UL, uses UL resources, or creates conflict-of-interest, reputational, financial, contractual or compliance exposure, those risks are **within scope** and must be identified and managed under UL policies.

### 1.3.3 Who is responsible for ensuring that the policy (and any associated procedure) is implemented and monitored?

The Governing Authority has a statutory obligation to provide for and maintain a risk management system within the University as part of an effective internal control system. The identification and management of risk are led on behalf of the University by the President, with support from the Executive Committee and UL's Risk Management Office.

Sections 5.1 and 5.2 below provide details on the various individuals and committees responsible for implementing and monitoring this policy. In addition, the Risk Management Division is responsible for maintaining supporting processes, templates, and guidance (including the Handbook), and for providing training, facilitation, and reporting to support consistent implementation.

**Definitions**

| | |
|---|---|
| **Risk** | The effect of uncertainty on UL's objectives. In the context of UL and its activities (and those of its subsidiaries/joint ventures), expressed as any positive or negative deviation from what is expected. Risk arises from events, conditions or decisions that may affect academic, research, operational, financial, compliance or reputational outcomes, and includes threats and opportunities (including missed opportunities). |
| **Controls** | Measures **in operation** that contain or modify risk. To be effective, a control must be in place, tangible, and designed to reduce the likelihood or impact of a risk. Controls include any process, policy, device, practice, or other condition in place to contain or modify risk. |
| **Actions** | Time-bound future measures that contain or modify a risk, reducing the likelihood or impact of that risk. Once completed, actions become controls. |
| **Risk treatment** | Selection and implementation of measures to modify risk (avoid, reduce, transfer, accept). This may include implementing effective controls and taking additional actions at the University. |
| **Inherent risk rating** | The risk level before control or action measures are in place |
| **Residual risk** | The risk that persists after considering existing controls |
| **Residual risk score** | The level of risk remaining after considering the effectiveness of existing controls, assessed UL's approved likelihood and impact scales and recorded in the RMIS. |
| **Target risk rating** | The planned level of risk, aligned with risk appetite |
| **Risk appetite** | The amount and type of risk UL is willing to accept in pursuit of its strategic objectives. It influences the University's operating style. |
| **Risk tolerance** | The permissible deviation from risk appetite in defined contexts |
| **Fundamental Risk Register (FRR)** | The central register of UL's most significant strategic/institutional-level risks – risks with the capacity to affect mission, strategic objectives, governance, reputation, financial sustainability and statutory compliance. The FRR is maintained by the Executive Committee (facilitated by the Risk Management Officer) and reviewed by the Audit & Risk Committee and Governing Authority at least twice yearly (minimum. |

## 2. Policy Statement

UL is committed to a proactive, structured enterprise risk management system integrated into governance and decision-making, consistent with the Code of Practice for the Governance of State Bodies (2016) and the Universities Act 1997 (as amended); and aligned to ISO 31000 principles. The system operates within the Risk Appetite Statement and delegated authority arrangements. UL will

A. maintain an enterprise risk management system that is integrated into planning, decision-making and performance cycles.

B. ensure all units maintain risk registers and review risks at a frequency proportionate to risk level but at least quarterly, and monthly for high/critical risks.

C. identify, assess and manage both threats and opportunities, comparing residual risk to risk appetite and escalating where thresholds are exceeded.

D. assign clear ownership for each risk, control and action, with accountability at the appropriate level.

E. maintain the Fundamental Risk Register (FRR) for UL's most significant risks, with Executive ownership and ARC/GA oversight at least twice yearly.

F. ensure risk is a standing agenda item for committee whose remit routinely involves material risks and that risk considerations and decisions are appropriately documented.

G. provide appropriate training, tools (RMIS), templates, and guidance to support consistent application across UL and its subsidiaries.

H. monitor and continually improve the risk management system through lessons from incidents, audits and reviews.

## 3. Context

### 3.1 Legal and Regulatory Context

The focus on governance in corporate and public bodies continues to increase. In developing this Enterprise Risk Management Policy, account has been taken of the following statutory and regulatory instruments:

- Code of Practice for the Governance of State Bodies (State Code) 2016
- Universities Act 1997 (as amended by the Higher Education Authority Act 2022)
- Joint Higher Education Authority (HEA) and Irish Universities Association (IUA) Report on the Governance of Irish Universities 2007
- ISO 31000 (2018) Risk Management Principles and Guidelines
- ISO 31050 Guidance for Managing Emerging Risks to Enhance Resilience (2023)

**As per the State Code, a risk management system involves**

- identifying risks that threaten the achievement of the University's objectives
- the evaluation of the likelihood of occurrence and potential impact of the risks identified
- the categorisation of risks according to their gravity
- the appraisal of controls/techniques and further steps to manage risks
- continual monitoring of the effectiveness of controls, management techniques and decision-making informed by the risk management process
- assessing residual risk levels and their acceptability

- establishing an audit and/or risk management committee and reporting to the Governing Authority to provide an independent view of risks and risk management systems
- making risk management a standing item on the agenda of the Governing Authority, the Executive Committee and other relevant subcommittees
- advising the Chancellor of the need to include risk management experience/expertise in the competencies of at least one Governing Authority member. Where the composition of the Governing Authority does not allow for this, expert advice should be sought externally.

### 3.2 Other Context

#### 3.2.1 Internal Documents

This policy relates to the following internal documents:

- Risk Appetite Statement
- Enterprise Risk Management Handbook
- Risk Assessment Template
- UL Safety Statement

#### 3.2.2 Health and Safety

A dedicated UL Health and Safety Risk Register was established to capture significant health and safety risks across the University. When completing health and safety risk assessments in collaboration with the Health and Safety section of HR, any risk that results in a residual risk rating of 8 or above must be escalated and recorded on the UL Health and Safety Risk Register.

Health and safety risks with a residual risk rating below 8 can be managed locally – either on the relevant local risk register or through local operational processes – in line with the University's health and safety management framework. This approach ensures that significant risks receive appropriate oversight at the institutional level while lower-level risks continue to be managed effectively within individual units, departments or areas.

## 4. How the Risk Management Framework Works

This section explains how UL's risk management system operates in practice, outlining the University's four organisational levels of risk oversight, the five core stages of the risk management process, the systems that support these activities, and how risk information moves through the institution to ensure effective identification, assessment, treatment, monitoring and reporting.

### 4.1 Risk Management Process Overview

UL's risk management operates through a continual cycle of activities that ensure risks are systematically identified, assessed, treated, monitored and reported. The process is relevant to multiple purposes, from individual projects and departments to faculties, divisions and the institution.

The diagram below provides a high-level visual representation of UL's Enterprise Risk Management (ERM) Framework. It illustrates the flow of risk information across the four levels of the institution, the specific steps involved at each stage, and the continual feedback loop that ensures improvement is ongoing.

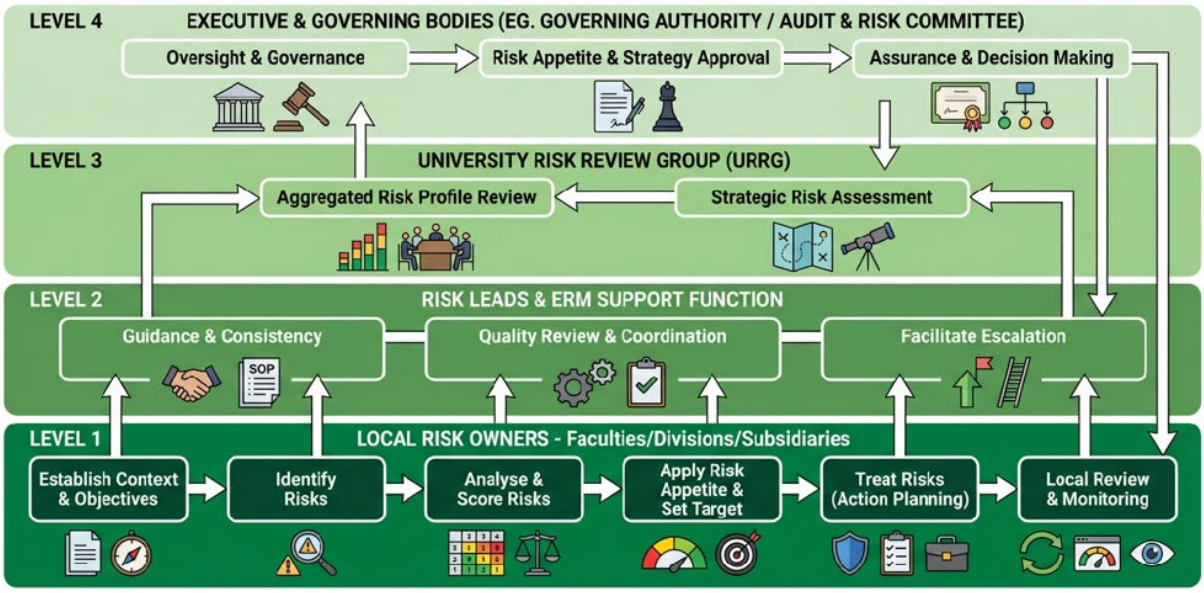



**Figure 4.1: UL ERM Framework**

## 4.2 Five Core Stages

The five core stages of the risk management process are

1. **Risk Identification**: Discovering and documenting potential risks once goals and objectives are identified
2. **Risk Analysis and Assessment**: Evaluating likelihood and impact
3. **Risk Treatment**: Implementing controls and actions
4. **Risk Monitoring**: Tracking effectiveness of treatments
5. **Risk Reporting**: Communicating risk status to stakeholders

### 4.2.1 Stage 1: Risk Identification

Risk identification is the first step in the University's risk management process. It involves recognising events, conditions or decisions that could affect the achievement of objectives, whether positively or negatively. Effective identification requires an understanding of what is trying to be achieved and an awareness of the internal and external factors that may influence those objectives. In practice, risks may be identified from a wide range of activities, including

- **Strategic planning exercises**: When developing or reviewing strategic plans, departmental objectives or business cases
- **Operational activities**: Day-to-day observations by staff of potential threats or opportunities
- **Incident and near-miss reporting**: Learning from events that have occurred or almost occurred
- **Internal and external audits**: Recommendations from audit findings
- **Stakeholder consultation**: Feedback from students, staff, partners and external bodies
- **Environmental scanning**: Monitoring regulatory changes, sector developments and emerging threats
- **Project initiation**: Risk assessments conducted at the start of significant projects or initiatives
- **Risk workshops and brainstorming sessions**: Facilitated sessions with key stakeholders

Everyone at UL has a responsibility to identify risks:

- **All staff** identify risks within their working environment and report them to their line manager.
- **Line managers** identify risks affecting their teams and operations.
- **Heads of departments/units** identify risks to achieving their strategic and operational objectives.
- **Faculty/divisional leadership** identify faculty/division-wide and cross-cutting risks.
- **Executive Committee members** identify institutional-level strategic risks.

Identified risks must be recorded in the RMIS (or escalated to a manager for recording) where they meet the materiality/escalation criteria in this policy.

-

Once identified, risks are recorded in

- **Local Risk Registers**: Maintained by departments, schools, units and faculties/divisions
- **Fundamental Risk Register (FRR)**: UL's central register for strategic and institutional-level risks
- **Health & Safety Risk Register**: Dedicated register for significant health and safety risks (residual rating ≥8)
- **Project Risk Registers**: For specific projects or initiatives

All risk registers are maintained using UL's **One Advanced Risk Management System** (UL Risk Management Information System RMIS), a centralised digital platform that ensures consistency, tracking and reporting capabilities.

#### 4.2.2 Stage 2: Risk Analysis and Assessment

**Step 1: Describe the Risk**

For each identified risk, document the

- **risk title**: A clear, concise description
- **risk description**: Detailed explanation of the risk event and its context
- **causes**: What could trigger this risk?
- **consequences**: What would happen if the risk materialised?
- **risk category**: Classification (see Table 5.1 in section 5.3): Strategic, Operational, Health & Safety, Financial and Reputational
- **risk owner**: The individual accountable for managing this risk

**Step 2: Assess Inherent Risk (Before Controls)**

If no controls were in place, determine the **likelihood** and **impact** of the risk occurring.

Likelihood scale (probability):

- **1 – Rare:** May occur only in exceptional circumstances (once in 5-10 years)
- **2 – Possible:** Could occur at some point (once in 3-5 years)
- **3 – Likely:** Likely, may occur (once every 1-2 years)
- **4 – Very Probable:** Very Likely, will occur in most circumstances (within the next year)

Impact Scale

- **1 – Minor:** Minimal impact on operations, objectives or reputation
- **2 – Moderate:** Some disruption but manageable
- **3 – Serious:** Significant impact requiring considerable management attention
- **4 – Extreme:** Catastrophic impact threatening strategic objectives or operations

| Inherent Risk Rating = Likelihood × Impact |
|---|

This produces a score from 1 to 16, which maps to one of the following risk levels:

- **1-3:** Low Risk (Green)
- **4-6:** Medium Risk (Yellow)
- **8-12:** High Risk (Orange)
- **12-16:** Critical Risk (Red)

**Step 3: Identify Existing Controls**

Document all current measures in place to manage the risk. Controls must be

- **tangible**: Concrete, specific measures (not vague statements)
- **in place**: Currently operational (not planned)
- **effective**: Actually working to reduce the likelihood or impact

**Examples of effective controls:**

- Policies, procedures and protocols
- Training and competency requirements
- Physical security measures (locks, access controls, fire systems)
- Financial controls (approval limits, segregation of duties)
- Insurance coverage
- Monitoring systems and audits
- Contractual protections

**Step 4: Assess Residual Risk (After Controls)**

Re-evaluate the **likelihood** and **impact** by considering the effect of existing controls:

| Residual Risk Rating = Likelihood (after controls) × Impact (after controls) |
|---|

This represents the current level of risk exposure and should be compared against UL's Risk Appetite Statement to determine if further action is required.

**Step 5: Set Target Risk Rating**

Based on the residual risk rating and the Risk Appetite Statement, ask these questions:

- **Is the residual risk acceptable?** If yes, target = residual (risk is within appetite)
- **Is further treatment needed?** If yes, set a target risk rating that aligns with UL's risk appetite

- Where residual risk is accepted, acceptance must be recorded and approved at the appropriate level in accordance with delegated authority and escalation requirements.

**Step 6: Develop Additional Actions (if Required)**

If the residual risk exceeds UL's risk appetite, develop specific actions to further reduce the risk:

- **Action description**: What will be done?
- **Action owner**: Who is responsible?
- **Deadline**: When will it be completed?
- **Expected impact**: How will this reduce the likelihood or impact?

Actions are tracked to completion in the One Advanced system. Once completed, actions become controls, and the residual risk rating is recalculated.

### 4.2.3 Stage 3: Risk Treatment

Risk treatment involves selecting and implementing measures to modify risk. UL adopts four primary treatment strategies, as specified in the table below.

**Table 4.1: Treatment strategies**

| Treatment strategy | Description | When to use | Example |
|---|---|---|---|
| 1. Avoid | Eliminate the risk by deciding not to proceed with the activity | When risk exceeds appetite and cannot be adequately controlled | Cancelling a high-risk event or discontinuing a problematic partnership |
| 2. Reduce/Mitigate | Implement controls or actions to lower the likelihood or impact | Most common approach; used when risk can be managed to acceptable levels | Installing fire suppression systems, implementing staff training, and enhancing cybersecurity |
| 3. Transfer | Shift risk to a third party | When another party can better manage the risk or when cost-effective | Purchasing insurance, outsourcing services with contractual protections, and using indemnities |
| 4. Accept | Deliberately retain the risk without further action | When residual risk is within appetite or the cost of treatment exceeds the benefit | Accepting minor operational inconveniences, tolerating acceptable levels of student complaints |

When selecting the right strategy, the choice depends on

- the residual risk rating versus UL's risk appetite
- cost-effectiveness of treatment options
- Practical feasibility of implementing controls
- timeframes for action
- regulatory or legal requirements
- **risk interdependencies** and **cumulative risk** exposure: including knock-on impacts across units, shared dependencies (e.g., key systems, suppliers, critical roles) and the aggregate effect of multiple risks materialising concurrently
- **non-tradeable constraints:** risks relating to **compliance, ethics, health and safety, and material reputational harm** cannot be offset by potential strategic or financial benefits and

must be treated and/or escalated in accordance with the escalation framework where thresholds are approached or exceeded

#### 4.2.4 Stage 4: Risk Monitoring

**Ongoing Monitoring Activities**

Once risks are assessed and treated, they require continual monitoring to ensure

- controls remain effective and are operating as intended
- actions are progressing to completion on schedule
- risk ratings remain accurate as circumstances change
- new risks emerge and are captured

**Monitoring Mechanisms**

Monitoring mechanisms include risk register reviews, standing agenda items, incident and near-miss reporting, audit and assurance activities, and key risk indicators.

1. Risk register reviews:
   - **Quarterly minimum** for all active risks
   - **Monthly** for high and critical risks
   - **After significant events** or changes to operations

2. Standing agenda item:
   - Risk management should be a standing item on departmental, faculty/divisional and committee meeting agendas.
   - Each meeting should review risk status, discuss emerging risks and confirm control effectiveness.

3. Incident and near-miss reporting:
   - All incidents and near misses are reported through UL's reporting system.
   - The Risk Management Officer performs trend analysis to identify systemic issues.
   - Incidents trigger risk register reviews to assess if risk ratings require updating.

4. Audit and assurance activities:
   - Internal audits test control effectiveness.
   - External audits provide independent validation.
   - Audit findings feed back into risk assessments.

5. Key risk indicators:
   - Key Risk Indicators (KRIs): Quantifiable metrics that provide early warning signals of increasing risk exposure or control weaknesses (e.g. frequency of cyber incidents, research funding decline, student retention rates, and health and safety incidents)
   - **Ownership and accountability:** For risks rated **High or Critical**, the **risk owner is responsible for defining appropriate KRIs**, ensuring they are measurable, monitored and reviewed at an agreed frequency.
   - **Reporting and escalation:** KRIs must be reported through the relevant risk register and governance forums and must inform escalation where adverse trends indicate that risk may exceed appetite, tolerance or delegated authority thresholds.

**When to Update Risk Assessments**

Risk assessments must be reviewed and updated when

- a risk materialises (incident occurs)
- controls are implemented or removed
- actions are completed
- new information emerges about the likelihood or impact
- organisational or operational changes occur (new systems, procedures, resources)
- external environment changes (new regulations, sector developments)
- risk owner or organisational structure changes

### 4.2.5 Stage 5: Risk Reporting

The purpose of risk reporting is to ensure that material risks are communicated promptly to the appropriate level of management or governance for review, decision-making and oversight.

**Table 4.2: Reporting structure and frequency**

**Risk Reporting & Escalation Schedule**
Minimum reporting cadence and content by level

| Level | Report from | Report to | Frequency | Content |
|---|---|---|---|---|
| Operational/ Local | Department/ Unit heads | Faculty/ Divisional Management | Quarterly (minimum) | Local risk register summary, high-priority risks, control effectiveness, and incidents |
| Faculty/ Divisional | Faculty/ Divisional Leadership | Executive Committee, UL Risk Review Group | Yearly/as necessary | Consolidated divisional risks, escalated risks, trends, and assurance on control effectiveness |
| Institutional | Executive Committee, Risk Management Officer | Audit & Risk Committee, Governing Authority | Twice yearly (minimum) | FRR review, risk appetite alignment |
| Project-specific | Project managers | Project sponsors | As per project governance | Project risk register, critical risks, issues impacting delivery |

**Escalation Criteria**

Risks should be escalated to the next management level when

- residual risk rating is High (8-12) or Critical (12-16)
- risk exceeds the Risk Appetite Statement thresholds
- risk has cross-cutting implications affecting multiple areas
- controls are inadequate or failing
- significant incidents have occurred
- strategic objectives are threatened
- external reporting or regulatory notification is required

**Fundamental Risk Register (FRR)**

The FRR is UL's central register of strategic and institutional-level risks. It includes

- risks with university-wide impact
- strategic risks threatening UL's mission or objectives

- compliance, governance and reputational risks at the institutional level
- risks escalated from faculties/divisions due to severity or cross-cutting nature

**FRR Governance**

- **Maintained by:** Executive Committee (facilitated by Risk Management Officer)
- **Reviewed by:** Audit & Risk Committee and Governing Authority
- **Frequency:** Twice yearly (minimum), with interim updates as required

## 4.3 Tools and Systems

**Risk Management Information System (RMIS)**

UL deploys a RMIS as its centralised risk management digital platform. This system provides

- centralised risk registers for all levels (local, faculty/divisional, institutional)
- standardised risk assessment templates to ensure consistency
- automated workflows for risk review reminders and escalation
- action tracking to monitor completion of mitigation measures
- reporting dashboards for management and governance oversight
- incident and near-miss reporting with trend analysis
- integration with other UL systems, where applicable

**Access and Training**

- Risk owners and managers receive training on the use of One Advanced.
- The Risk Management Division provides ongoing support and guidance.
- User guides and templates are available on the UL Risk Management website.

**Supporting Documentation**

To support implementation, UL provides

- **Enterprise Risk Management Handbook**: Detailed guidance on risk management processes
- **Risk Assessment Template**: Standardised format for documenting risks
- **Risk Appetite Statement**: Defines acceptable risk levels by category
- **Risk Register templates**: For local, project and divisional use
- **Training materials and workshops**: Delivered by the Risk Management Division

## 4.4 Practical Workflow Example: From Risk Identification to Closure

**Scenario:** A Principal Investigator (PI) identifies a risk that inconsistent data documentation practices within a research project may compromise research integrity and the reliability of research outputs. The step-by-step workflow is given below.

1. **Identification (Week 1)**
   - The PI raises the concern during a project meeting.
   - Risk is logged in the local risk register via the RMIS.
   - Following consultation, the Head of Department agrees to act as risk owner, given the implications for research integrity within the faculty.

2. **Analysis and Assessment (Week 2)**
   - Risk owner conducts analysis:

    - **Causes**: Inconsistent data recording practices; insufficient documentation standards; varied approaches across team members; inadequate onboarding of new researchers
    - **Consequences**: Difficulty verifying findings; potential funder non-compliance; reputational impact, risk of publication delays and/or corrections to already published material
- **Inherent risk**: Likelihood = 3 (Likely), Impact = 4 (Extreme) → Rating = 12 (High)
- **Existing controls**: Research Integrity Policy, data management plans, supervisor oversight, mandatory training
- **Residual risk**: Likelihood = 2 (Possible), Impact = 4 (Extreme) → Rating = 8 (High)

**3. Treatment Planning (Week 3)**

- **Residual risk** (8) exceeds risk appetite for research integrity and compliance risks
- **Target risk**: Rating = 4 (Medium), Likelihood = 2, Impact = 2
- Actions developed:
    - Action 1: Deliver targeted data management training to the research team (Owner: PI, deadline: 1 month)
    - Action 2: Implement enhanced, consistent research documentation and record-keeping protocols across the project (Owner: Faculty Research Office, deadline: 2 months)
    - Action 3: Conduct an internal review of data documentation practices (Owner: Research Integrity Officer, deadline: 2 months)

**4. Escalation (Week 4)**

- Due to the nature of research integrity risks, the risk is escalated to the **Faculty Risk Register**.
- Faculty leadership reviews the risk and escalates to UL Risk Review Group (ULRRG)
- ULRRG determines that the risk does not meet the criteria for escalation to the Fundamental Risk Register (FRR) because the impacts are currently contained within the faculty and can be effectively managed through the actions underway.
- ULRRG recommends that the risk continue to be monitored and managed at faculty level, with regular progress updates.

**5. Reporting (Ongoing)**

- Risk owner provides monthly updates to Faculty Research leadership
- Faculty Research leadership continues to monitor progress on the effectiveness of controls and execution of future actions.
- The risk is not included on the FRR and remains under faculty-level oversight.

**6. Monitoring (Months 1–4)**

- Action 1 completed in Month 1; training uptake is high and immediate practices improve.
- Action 3 identifies further documentation inconsistencies, which are resolved.
- Reassessment after two months: Likelihood = 2 (Possible), Impact = 3 (Serious) → Rating = 6 (Medium).
- The risk remains under review until the documentation protocol is fully embedded.

**7. Closure (Month 7)**

- All actions are completed: standardised documentation protocol is implemented; training delivered; internal review actions closed.
- Final assessment: Likelihood = 1 (Unlikely), Impact = 3 (Serious) → Rating = 3 (Low).

- The risk is now within appetite and is retained on the Faculty Risk Register with quarterly monitoring.

**8. Continual Review (Ongoing)**

- Quarterly reviews ensure controls remain effective.
- If no further issues arise, risk may be de-escalated to the local register.

### 4.5 Key Success Factors

For UL's risk management framework to operate effectively, the following elements are essential:

✅ **Leadership commitment**: Executive and senior management visibly support risk management.
✅ **Clear accountability**: Every risk has a designated owner who is responsible and empowered.
✅ **Risk-aware culture**: All staff understand their role and feel comfortable raising concerns.
✅ **Integration**: Risk management is embedded in planning, decision-making and operations (not a separate exercise).
✅ **Practical tools**: One Advanced system and templates make risk management accessible.
✅ **Regular communication**: Risk is discussed openly at all levels through standing agenda items.
✅ **Training and support**: Risk Management Division provides guidance and builds capability.
✅ **Continual improvement**: Lessons learned from incidents and audits feed back into the system.
✅ **Appropriate resources**: Sufficient time, budget and personnel are allocated to risk management activities.

**Assurance and testing of controls:** Controls and mitigations are subject to periodic testing, review and independent assurance (where appropriate) to confirm that they are designed effectively, operating as intended and remain proportionate to the level of risk.

# 5. Related Procedures for Enterprise Risk Management

## 5.1 Overview of Risk Management at UL



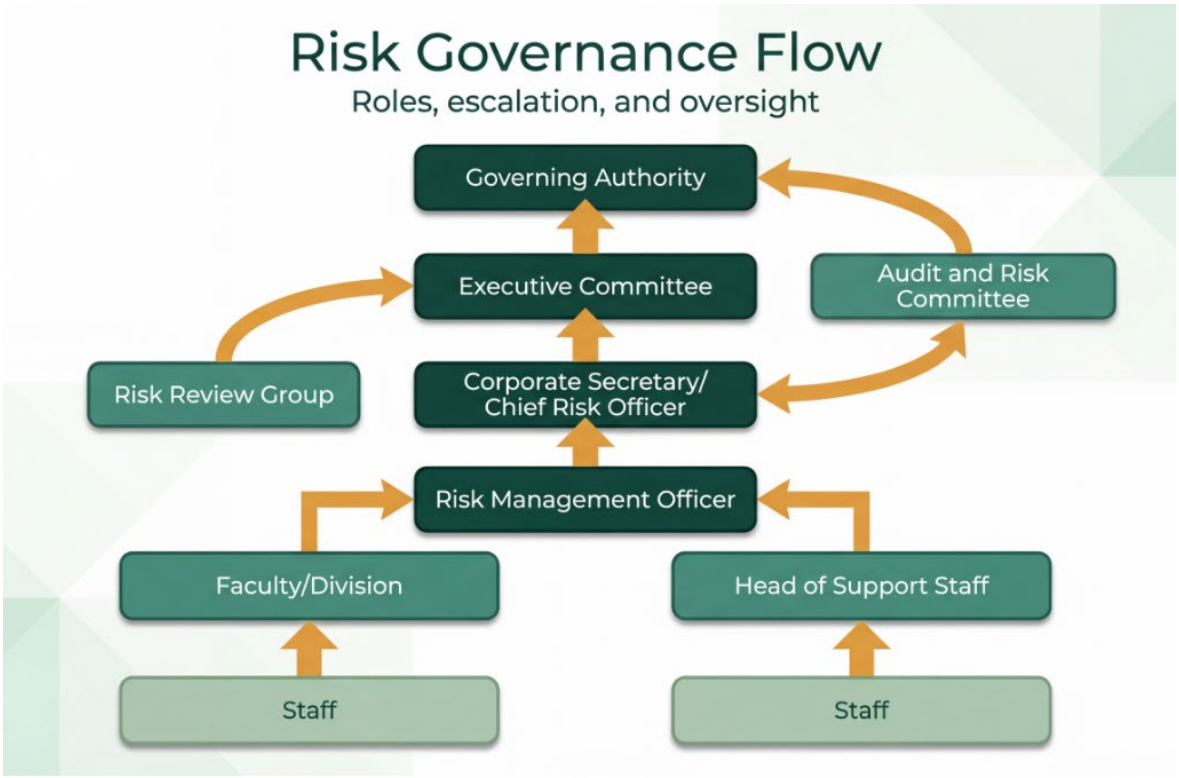




**Figure 5.1: Overview of risk management at UL**

## 5.2 Roles and Responsibilities

| | |
|---|---|
| **Governing Authority** | The Governing Authority (GA) is accountable to the HEA and the Department of Further and Higher Education, Research, Innovation and Science for the funding it receives. As described in the State Code, the GA fulfils key functions regarding the University, including providing for and maintaining a risk management system. The GA is responsible for reviewing the Fundamental Risk Register twice a year. |
| **Audit and Risk Committee and other GA committees** | The GA Audit and Risk Committee (ARC) is responsible for providing oversight and advice to the GA concerning the operation of this policy. As assigned by the GA and in consultation with the ARC, other GA committees provide oversight of specific risks relevant to their area(s) of responsibility. The ARC is responsible for reviewing the Fundamental Risk Register twice a year. |
| **President and Executive Committee** | Led by the President, the Executive Committee is responsible for executive decision-making in the University. This includes implementing and ensuring compliance with this policy. The Executive Committee is responsible for reviewing the Fundamental Risk Register twice a year. |
| **Corporate Secretary** | As part of their role, the Corporate Secretary performs the functions of the Chief Risk Officer and, in this capacity, reports directly to the GA and ARC. The Chief Risk Officer oversees the identification, assessment and mitigation of risks to ensure UL's stability, support compliance and promote a risk-aware culture throughout UL. |
| **Risk Management Officer** | The Risk Management Officer reports directly to the Corporate Secretary and supports the identification, assessment and oversight of risk, including monitoring and reporting risk and promoting a risk management culture throughout UL. Under the direction of the Corporate Secretary, the Risk Management Officer trains people to identify risks, assists with risk rating, coordinates reviews of this policy and the Enterprise Risk Appetite Statement, manages and monitors the risk incident and near-miss reporting processes, and performs trend analysis of all reported incidents. |
| **UL Risk Review Group** | The UL Risk Review Group (ULRRG) aims to enhance the execution of campus strategic and operational risk management and provide comprehensive risk reporting to support the UL strategic plan. The ULRRG ensures a consistent approach is taken to project delivery and helps manage associated operational risks. Additionally, it serves as a point of contact for operational risks with campus-wide implications and assists the Executive Committee in overseeing organisational risks. The composition of the ULRRG is agreed by the Executive Committee. The ULRRG operates under terms of reference approved by the Executive Committee and supports risk escalation, challenge and consistency of ratings and controls. |
| **Faculties and divisions with management responsibilities** | All employees with management responsibilities are responsible for<br>– implementing and ensuring compliance with this policy in their areas of responsibility<br>– ensuring that appropriate and effective risk management processes are in place within their areas of responsibility<br>– risk assessing all strategies, business plans and service developments, including changes to service delivery<br>– developing specific objectives within their service or operational plans that identify future risks |

| | |
|---|---|
| | – ensuring that a process for identifying risk is in place throughout all areas of responsibility and that risk assessments are conducted in accordance with this policy<br>– maintaining a risk register and formally reporting on risk to the next management level<br>– ensuring that staff within their remit identify risks in their working environment and are aware of their personal responsibilities in accordance with this policy |
| **Staff** | All staff are required to<br>– comply with this policy in relation to identifying and managing risk<br>– understand that risk management is integral to their academic/research/managerial practice within the University<br>– have knowledge of the related risk management procedures that support this policy<br>– identify and report any potential risks to their line manager<br>– complete risk management training appropriate to their role<br>While every staff member is responsible for identifying and managing risk in their work, certain common roles and responsibilities govern the communication, notification, and escalation of identified risks, controls, and actions. |
| **Subsidiary companies** | To ensure consistency and effective risk management, subsidiaries maintain their risk registers using UL's centralised One Advanced Risk Management system. Subsidiaries work closely with the Risk Management Division to embed robust risk management practices throughout their organisations, ensuring alignment with UL's standards and fostering a culture of proactive risk awareness and control. |

## 5.3 Categorising Risk

**Table 5.1: Categories by risk impact**

| Impact category | 1: Minor | 2: Moderate | 3: Serious | 4: Extreme |
|---|---|---|---|---|
| **Impact assessment criteria at the faculty and division level** | | | | |
| **Constituent strategy:**<br>**1. Research and Innovation**<br>**2. Teaching and Learning**<br>**3. International**<br>**4. Student Experience**<br>**5. Engagement** | Some delay in implementing a strategic objective or initiative | Significant delay in implementing a strategic objective or initiative | Failure to deliver on one or more of the strategic objectives or initiatives | Failure to deliver one or more of the mission's critical activities or strategic objectives |
| **Operational:**<br>**1. Physical Infrastructure**<br>**2. Unit Effectiveness** | Short-term disruption to a critical activity | Short-term significant disruption to critical activities | Ongoing and significant disruption to critical activities | Complete shutdown of critical activities for an extended period |
| **Health and Safety** | Minor injury or illness, first aid treatment required <3 days absence, 3 days extended hospital stay.<br>Impaired psychosocial functioning greater than 3 days, less than 1 month. | Significant injury requiring medical treatment e.g., fracture and/or counselling.<br>Agency reportable e.g., HAS, Gardaí (violent and aggressive acts) >3 days absence, 3 to 8 days extended hospital stay.<br>Impaired psychosocial functioning greater than 1 month, less than 6 months. | Major injuries/long-term incapacity or disability (loss of limb) requiring medical treatment and/or counselling.<br>Impaired psychosocial functioning for greater than 6 months. | Incident leading to death or major permanent incapacity.<br>Event has impact on large number of patients or members of the public.<br>Permanent psychosocial functioning incapacity. |
| **Financial** | Up to €300k | €300k to €750k | €750k to €1.5m | Above €1.5m |
| **Reputational** | Some negative comments in local press/media | Critical article in local media or criticism from within UL senior management | Continuing and significant publicity in local or national media regarding UL management | Unit loses the confidence of the public or UL management |

| Impact assessment criteria at the institutional level | | | | |
|---|---|---|---|---|
| **Constituent strategy:**<br>**1. Research and Innovation**<br>**2. Teaching and Learning**<br>**3. International**<br>**4. Student Experience**<br>**5. Engagement** | Some delay with achieving more than one of the constituent strategies, or a significant delay with a single constituent strategy | Significant delay in achieving more than one constituent strategy | Failure to deliver on one or more of the following constituent strategies:<br>– International<br>– Student Experience<br>– Engagement | Failure to deliver on one or more of the following mission-critical strategies:<br>– Teaching and Learning<br>– Research and Innovation |
| **Operational:**<br>**1. Physical Infrastructure**<br>**2. Unit Effectiveness** | Short-term disruption to a critical UL activity | Short-term and significant disruption to critical UL activities | Ongoing and significant disruption to critical UL activities | Complete shutdown of UL activities for an extended period |
| **Health and Safety** | Minor injury or illness, first aid treatment required <3 days absence, 3 days extended hospital stay.<br>Impaired psychosocial functioning greater than 3 days, less than 1 month. | Significant injury requiring medical treatment e.g., fracture and/or counselling.<br>Agency reportable e.g., HAS, Gardaí (violent and aggressive acts) >3 days absence, 3 to 8 days extended hospital stay.<br>Impaired psychosocial functioning greater than 1 month, less than 6 months. | Major injuries/long-term incapacity or disability (loss of limb) requiring medical treatment and/or counselling.<br>Impaired psychosocial functioning for greater than 6 months. | Incident leading to death or major permanent incapacity.<br>Event has impact on large number of patients or members of the public.<br>Permanent psychosocial functioning incapacity. |
| **Financial** | Up to €2m | €2m to €5m | €5m to €10m | Above €10m |
| **Reputational** | Adverse and widely reported media coverage about UL | Widely reported (but unproven) allegations of serious misconduct | Widely reported and proven mismanagement with Government review | Widely reported and proven mismanagement with Government sanction against UL or loss of public confidence |

### 5.4 Risk Appetite

Risk appetite is the level of risk UL is willing to accept to achieve its strategic objectives. The Governing Authority sets UL's risk appetite and articulates it through the approval of the Risk Appetite Statement.

The Risk Appetite Statement defines the appetite for risk and tolerance for specific risk areas. UL may be risk-taking or risk-averse, and its willingness to accept risk varies by risk type.

For more information, refer to the UL Risk Appetite Statement on the Policy Hub.

## 5.5 Risk Management Cycle

The Risk Appetite Statement should always be used in conjunction with the risk cycle outlined below.

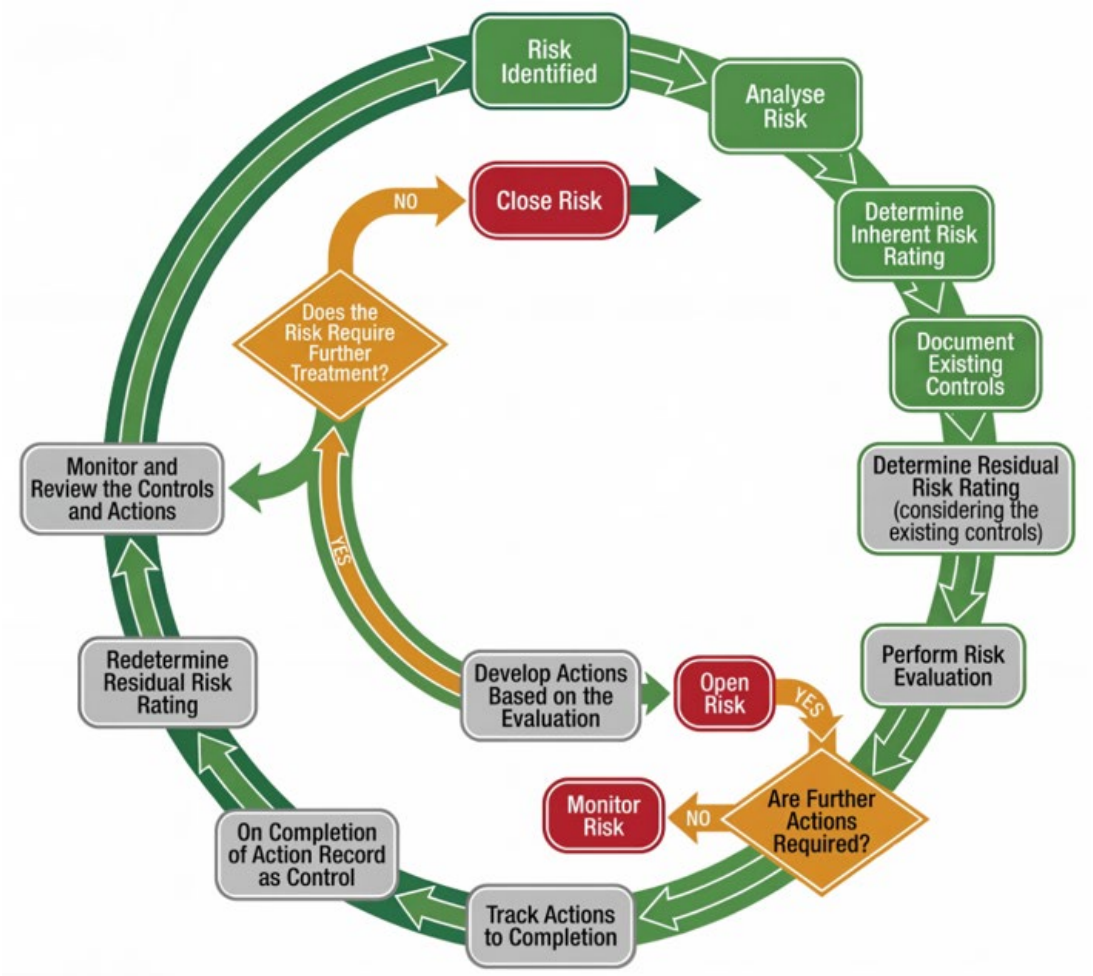



**Figure 5.2: Risk management cycle**

The risk management cycle is illustrated in the table that follows.

**Table 5.2: Steps involved in the risk management cycle**

| Step | Details |
|---|---|
| **1. Risk identified** | The risk of a fire in a laboratory |
| **2. Analyse risk** | Potential causes: Flammable chemicals, electrical faults, equipment overheating, human error |
| | Potential consequences: Injury or loss of life, damage to property, loss of research data, interruption to research |
| **3. Inherent risk rating** | Likelihood: 3 |
| | Impact: 4 |
| | Inherent risk rating: 12 (high) |
| **4. Document existing controls** | Fire alarms and smoke detectors |
| | Fire extinguishers |
| | Fire suppression systems (e.g., sprinklers) |
| | Safety training for all lab personnel |
| | Proper storage of flammable substances |
| | Regular inspections and maintenance of electrical equipment |
| | Emergency evacuation plans |
| **5. Residual risk rating** | Likelihood: 2 |
| | Impact: 3 |
| | Residual risk rating: 6 (medium) |
| **6. Performance risk evaluation** | Effectiveness of controls: Regularly tested and effective |
| | Incident history: No recent incidents |
| | Compliance with regulations: Full compliance |
| **7. Are further actions required?** | No: The risk is currently managed effectively with existing controls. |
| **8. Monitor and review** | Regular monitoring: Continue regular inspections, maintenance and safety drills. |
| | Review frequency: Quarterly reviews and after any near-miss or incident |
| **9. Does the risk require further treatment?** | No: Existing controls are sufficient to manage the risk effectively. |
| **Conclusion** | Close risk: The risk of fire in the laboratory is effectively controlled.<br>Accept and monitor at agreed frequency; close only where risk no longer exists. |
| **If Yes to further actions required** | Scenario example: An incident reveals that current chemical storage protocols are insufficient. |
| | Develop actions: Improve protocols, provide additional training and update safety data sheets. |
| **Track actions to completion** | Assign responsible personnel, set deadlines and monitor progress until completion. |
| **Record as control** | Document new controls and integrate them into the lab's safety procedures. |
| **Redetermine residual risk rating** | Likelihood: 1 |
| | Impact: 2 |
| | New residual risk rating: 1 x 2 = 2 (low) |
| **Monitor and review** | Continual monitoring: Ensure new controls are functioning as intended. |
| | Regular reviews: More frequent initially, then revert to standard frequency. |
| **Does the risk require further treatment?** | No: If new measures are effective, the risk can be closed. |
| | Yes: If further issues are identified, continue developing actions based on evaluation. |

## 5.6 Managing Risk

Once risks have been identified, recorded, and analysed, and agreed treatments have been implemented, managers need to establish a process for reviewing risk profiles and activities in their area of responsibility. An appropriate monitoring and reporting regime should be established to track the treatment's effectiveness in controlling the risk.

Risk management must be a standing agenda item at relevant management and committee meetings where material risks are routinely considered. Regular reviews aim to identify new risks and monitor existing ones to ensure that controls remain effective and appropriate, and that actions are completed as required. At a minimum, risks must be reviewed quarterly, with more frequent reviews for high/critical risks, or as required by appetite/tolerance.

In addition, risk assessments should be reviewed if the service or organisation changes, such as when new resources or procedures are introduced that would impact the risk. Changes made to the risk assessment should be brought to the attention of relevant staff and others.

This ongoing review helps ensure that risks are identified and managed. Such assurances are seen as part of the University's lines of defence. Implementing tangible mitigations and controls is crucial within the risk management system because they provide concrete measures to prevent, minimise, or eliminate potential threats. This ensures operational/organisational stability, whereas vague or poorly defined controls or mitigations are ineffective.

## 5.7 Risk Management Model

As illustrated below, UL's risk management model comprises Governing Authority oversight; three levels of internal management (Executive Committee, Risk Management Division, and internal audit function); and external auditors.

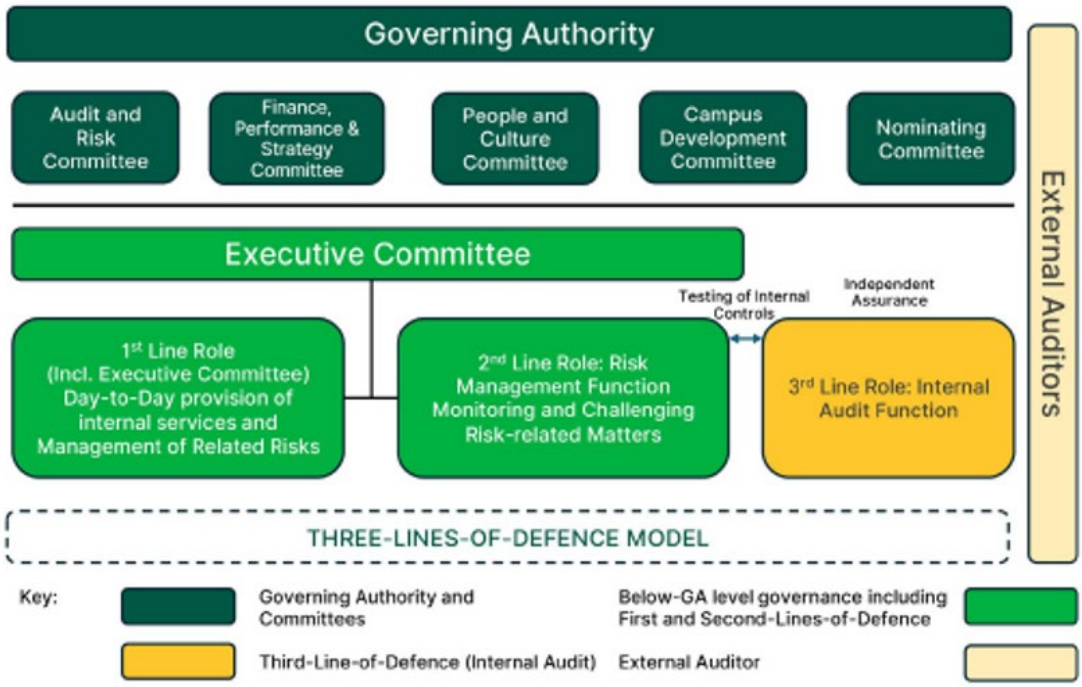



**Figure 5.3: UL risk management model**

**The Governing Authority**

- holds statutory responsibility for the **oversight** of the University and its system of internal control, including risk
- approves the enterprise risk management strategy and ensures it aligns with the institutional strategy and goals
- nurtures a culture that promotes ethical behaviour and accountability
- ensures that appropriate governance structures and committees (including the Audit & Risk Committee) are in place to support effective oversight
- delegates or assigns responsibility in a manner that supports the Chief Risk Officer and senior management in achieving the objectives of the University
- decides upon the University's appetite for risk in relation to the opportunities that come with the assumption of such risk and oversees risk management
- maintains oversight of compliance with legal, regulatory and ethical expectations

**As the first line of defence, the Executive Committee**

- leads and directs actions (including managing risk) and the application of resources to achieve the University's objectives
- maintains an ongoing dialogue with the Governing Authority and reports on planned, actual and expected outcomes linked to the University's objectives and risk
- establishes and maintains appropriate structures and processes for managing operations and risk
- ensures compliance with legal, regulatory and ethical expectations

**As the second line of defence, the Risk Management Division**

- provides expertise and support, conducts monitoring and identifies challenges relating to the management of risk, including
- supporting the development, implementation and continual improvement of risk management practices at process, systems and entity levels
- supporting the achievement of risk management objectives, such as compliance with laws, regulations and acceptable ethical behaviour; internal control; information and technology security; sustainability; and quality assurance
- provides analysis and reports on the adequacy and effectiveness of risk management

**As the third line of defence, the internal audit function**

- maintains primary accountability to the Governing Authority and is independent from management responsibilities
- communicates independent and objective assurance and advice to management and the Governing Authority on the adequacy and effectiveness of governance and risk management to support the achievement of UL's objectives and to promote and facilitate continual improvement
- reports impairments to independence and objectivity to the Governing Authority and implements safeguards as required

**External auditors provide additional assurance to**

- satisfy legislative and regulatory expectations that protect stakeholders' interests
- satisfy requests by management and the Governing Authority to complement internal sources of assurance

## 6. Related Documents

- Enterprise Risk Appetite Statement
- Enterprise Risk Management Handbook
- Risk Assessment Template
- Health & Safety documents, including UL Safety Statement

## 7. Document Control

| | |
|---|---|
| Document Version | Version 3.0 |
| Document Owner | Corporate Secretary's Office |
| Approved by | Executive Committee |
| Date | 18 February 2026 |
| Approved by | Audit and Risk Committee |
| Date | 6 March 2026 |
| Approved by | Governing Authority |
| Date | 26 March 2026 |
| Effective Date | 26 March 2026 |
| Scheduled Review Date | 26 March 2028 |