#

**Risk Management**

**Guidance Manual**

Sep 2022

# FORWARD

Risk is the effect of uncertainty on objectives. It is inherent in everything we do. It is what brings both hazards and opportunity to our lives and work. Every morning when we start our day, we instinctively consider the risks along the way; will there be snow, requiring us to leave early for work so as not to be late? Alternatively, will the roads be clear, allowing us to spend a bit more time with the children over breakfast? Routine activities like those we encounter daily in life and work do not need a lot of formal risk management; we have internalized those processes to such an extent that they have become second nature. The potential impacts of risk within the University of Edinburgh’s context, however, are often more severe than being late for work.

Students, staff, our city, nation and indeed the world at large look to us to provide meaningful impact for society. They expect and deserve enlightened education programs, world-class research and first class professional services, within an environment that encourages innovation and treats everyone with respect. They expect facilities that are fit for purpose, accessible and safe. These objectives are critical to our continued existence as an educational and research centre of excellence. As a result, a more formal approach to risk management is appropriate.

When examining the risks associated with achieving the goals and objectives of the University, it is important to first ask, “How do existing legislation, regulations, and current policies and practice guide how we do business?” Numerous policies and controls are in place to manage known risks. Initially, the most effective risk management technique is often compliance with these pre-existing policies and controls. This does not mean blindly following how we have always done things; this is the antithesis of innovation. Rather, it is only when we operate from a known and defined baseline that modifications can be consciously and responsibly considered.

Next, ask:

1. **What are we trying to achieve?** This could be an Area of Focus or objective from Strategy 2030; a supporting planning submission; or local goal, objective, performance measure or milestone identified in a project or work plan.
2. **What Risk Events** might impact our achievement of the goal? While our minds often default to negative events or obstacles, a risk event is something that might happen to prevent success, or an unexpected opportunity worth pursuing.
3. **What Causes** might bring about the risk event? There are often multiple factors or triggers, acting alone or in concert, that could bring about a risk event.
4. **What Impacts** **or consequences** would be felt should the event come to pass? This could vary from minor adjustments to a plan or budget, to the unrecoverable failure of a major initiative, or even loss of life.
5. **What existing controls** are in place to change the likelihood of the event (usually by addressing a cause), or mitigate the severity of the impact, should the event occur?
6. **Are existing controls sufficient**, or should we do more? If “more”;
7. **What additional actions are required**, who’s responsible for their delivery, and by what date?

Risk management helps answer these questions and provides a process by which anyone can identify and assess the risks; evaluate them; develop prevention, mitigation and recovery strategies; and ultimately achieve their goals most efficiently.

This guidance manual and the companion [*BS/ISO 31000:2018 Risk Management –Guidelines*](https://bsol-bsigroup-com.ezproxy.is.ed.ac.uk/Bibliographic/BibliographicInfoData/000000000030315447)provides the direction and process for standardizing the risk management practice at the University of Edinburgh to help us achieve our goals and objectives, and maintain the University’s long standing as one of the best research and teaching institutions in the world.

Contents

[FORWARD 1](#_Toc511375224)

[SECTION 1 – GENERAL 4](#_Toc511375225)

[1.1 VISION 4](#_Toc511375226)

[1.2 SCOPE 4](#_Toc511375227)

[1.3 AUDIENCE 4](#_Toc511375228)

[1.4 HOW TO USE THIS GUIDELINE 4](#_Toc511375229)

[1.5 OBJECTIVES 5](#_Toc511375230)

[SECTION 2 –RISK MANAGEMENT 6](#_Toc511375231)

[2.1 RISK MANAGEMENT FRAMEWORK 6](#_Toc511375232)

[2.2 POLICY 7](#_Toc511375233)

[2.3 ROLES AND RESPONSIBILITIES 7](#_Toc511375234)

[2.4 ADDITIONAL INFORMATION 9](#_Toc511375243)

[SECTION 3 – APPLICATION OF RISK MANAGEMENT PROCESS 10](#_Toc511375244)

[3.1 GENERAL 10](#_Toc511375245)

[3.2 COMMUNICATE AND CONSULT 10](#_Toc511375246)

[3.3 ESTABLISH THE CONTEXT 11](#_Toc511375247)

[3.3.1 Specialized Contexts: Sub-disciplines within Risk Management 13](#_Toc511375248)

[3.4 IDENTIFY RISKS 13](#_Toc511375249)

[3.4.1 Risk Identification Methods: 13](#_Toc511375250)

[3.4.2 How to State Risks 14](#_Toc511375251)

[3.4.3 Existing Controls 15](#_Toc511375252)

[3.5 ANALYZE RISK 15](#_Toc511375253)

[3.5.1 Risk Rating 15](#_Toc511375254)

[3.5.2 Risk Rating Terms 17](#_Toc511375255)

[3.6 EVALUATE RISK: EXISTING CONTROLS, RISK APPETITE 18](#_Toc511375256)

[3.7 ACTIONS REQUIRED: TREAT THE RISK 18](#_Toc511375257)

[3.7.1 Diversity of Risk Treatment (Mitigation) 19](#_Toc511375258)

[3.7.2 Ensuring Effective Risk Treatment (Mitigation) 19](#_Toc511375259)

[3.8 MONITOR AND REVIEW 20](#_Toc511375260)

[3.8.1 Monitor: Regular Management of Risk Information 20](#_Toc511375261)

[3.8.2 Review: Historical Risk Information 20](#_Toc511375262)

[3.9 RECORD THE RISK MANAGEMENT PROCESS 20](#_Toc511375263)

[APPENDIX 1 – ENTERPRISE RISK MANAGEMENT CULTURE: 22](#_Toc511375264)

# SECTION 1 – GENERAL

## 1.1 VISION

The University of Edinburgh pushes the boundaries of knowledge, innovating and implementing strategic developments; accepts that risk is inherent in doing so while taking prudent steps to manage this risk through optimal monitoring, treatment, and transfer; and consciously retains residual risk at an appropriate level to protect our reputation and sustainability.

## 1.2 SCOPE

This document replaces the University of Edinburgh’s Risk Management Guidance Manual 2010, which is hereby withdrawn. University of Edinburgh *Risk Policy and Risk Appetite Statement* makes mandatory the establishment and application of risk management across the University. This Risk Management Guidance Manual establishes the application of risk management within Colleges and Professional Services Groups. Subsidiary companies and autonomous organizations such as the Students’ Association are encouraged to review this guideline and apply the contents as appropriate.

## 1.3 AUDIENCE

This guideline serves primarily University employees having risk management responsibilities. It is also a useful reference for those wishing to incorporate the risk management process into business planning, project management, procurement, service delivery and policy development.

## 1.4 HOW TO USE THIS GUIDELINE

This Risk Management Guidance Manual assists in the application of the University’s risk management standard in all aspects of operations. The guideline is a companion to:

1. [***BS/ISO 31000: 2018 Risk Management –Guidelines***](https://bsol-bsigroup-com.ezproxy.is.ed.ac.uk/Bibliographic/BibliographicInfoData/000000000030315447)*(“the standard”*), is the international standard for risk management. It has been adopted by the University of Edinburgh and provides for the University’s risk management framework and process.
2. [***Risk Policy and Risk Appetite Statement***](https://www.ed.ac.uk/unpublished/corporate-services/risk-management/risk-management-information), provides risk management direction to the University’s Colleges and Professional Services Groups. It assigns specific risk management roles and responsibilities, establishes the Enterprise Risk Management (ERM) framework and policy throughout the University, and details specific risk management and reporting processes and tasks.
3. [***4Risk***](https://uoeriskmanagement.insight4grc.com/Risk/Home.aspx) is a secure cloud-based risk management application that is to be used across the University for all risk assessments, unless alternative prescribed formats are specifically required by legislation, regulation or Court-approved policy. It allows users to input risk information, identify and implement risk control strategies, monitor results, and report status and progress to date. Users must be granted access through the University Risk Manager. Email Chris.MacLean@ed.ac.uk for assistance.
4. [***Standard Risk Register Template***](https://www.ed.ac.uk/unpublished/corporate-services/risk-management/risk-management-information) is the University’s legacy risk register template. It is used by exception only, by select organizations or project teams within the university which do not fall easily within the existing governance and reporting structure.
5. ***Supporting tools and documents***, such as a Risk Dictionary, Likelihood and Consequences guide, and advice on loss reporting, indemnities, waivers of liability, and financial guarantees are available from the University Risk Manager, at chris.maclean@ed.ac.uk .

## 1.5 OBJECTIVES

The University’s risk management objectives are as follows:

1. Strategic level decision-making and planning are informed by accurate and congruent assessment of risk across the diverse Colleges, Groups, Major Programs and subsidiaries through formal University-wide Enterprise Risk Management (ERM) framework and processes.
2. Effective College, Group and subsidiary operational decision-making is guided by accurate and congruent assessment of risk within and across their diverse business areas. The risk management framework and process in place at this operational level supports and feeds back into the strategic level ERM framework, while meeting the needs of each distinct organization.
3. All risk management across the University adheres to the current risk management framework established by the Court, while encouraging a culture of innovation and opportunity, informed risk taking within the University’s risk appetite, and an acknowledgement of risk as inherent in all activities of the University.

# SECTION 2 –RISK MANAGEMENT

## 2.1 RISK MANAGEMENT FRAMEWORK

The University’s Risk Management Framework consists of the standards, policies, culture, responsibilities, and governance and reporting structures within which the risk management process is applied.

BS/ISO 31000:2018 defines the risk management process adopted by the University. Its application can be viewed on a continuum from the informal factoring of basic risk information into routine business decisions, to the formal conduct of detailed risk assessments as part of University-wide strategic planning. Regardless of scope, the process remains the same. Along the continuum of risk management, three basic perspectives emerge. These are Enterprise Risk Management (ERM); College, Group, and operational risk management; and the delivery of central risk management programs and services.

1. ***Enterprise Risk Management (ERM)****:* ERM describes the integrated and coordinated application of risk management congruently *across* Colleges, Groups and subsidiaries of the University, and *through* each organization, from Court, to colleges/groups, to schools, programs, projects, right down to the individual employee providing front-line service, teaching or research. In this context, *enterprise* implies the whole of the University –the full breadth and depth of everything we do.

A common risk management process applied across the University, combined with consistent risk reporting to executive and senior leaders will aid strategic decision-making, planning and resource allocation. ERM allows the leaders and executive to:

1. Identify risks that are shared across the University;
2. Apply combined risk mitigation strategies;
3. Determine overarching priorities;
4. Facilitate discussion of the types and levels of risk the University is prepared to accept (appetite and tolerance); and
5. Make long-term plans for the future.

2. ***College, Group and operational level risk management****:* risk management processes and policies applied within Colleges (and their constituent schools, centres and institutions), and Professional Services Groups (and their constituent service departments and teams). Operational risk management is focussed for the most part internally, to promote the success of internal College/School,and Group/Department goals and objectives. Being scalable, the basic risk management process is the same whether employed to inform the College and Group annual business and service plans, or to help inform a project or program plan.

Operational risk management also refers to areas of specialist risk that often have their own industry standards and professional practices and codes of conduct, such as accounting, audit, information technology, emergency management, physical security, procurement, and Health and Safety. While often guided by their own policies and procedures, they are integral to the University’s integrated risk management approach and as such, should be coordinated with the strategic ERM program.

***3. Central risk management programs and services****:* these are the programs and services offered by the Risk and Resilience team, resident in Corporate Services Group to address specific risk management needs of the University. Examples include:

1. risk management consulting and advisory services;
2. facilitation of risk assessments;
3. review of operational risk registers to find common themes, dependencies and solutions;
4. collation of operational risks for escalation and reporting to Court.

For more information on central risk management programs and services, visit the Risk

Management team website at <https://www.ed.ac.uk/corporate-services/risk-management>.

## 2.2 POLICY

The University of Edinburgh Court provides specific direction for risk management from the three perspectives: ERM; College, Group and operational risk management; and central risk management programs and services. It also sets the University’s Risk Appetite across numerous categories of risk, establishing the maximum level of acceptable risk across different domains of activities. Consult [*The University of Edinburgh Risk Management Policy and Risk Appetite Statement*](https://www.ed.ac.uk/sites/default/files/atoms/files/risk_policy_and_appetite_-_new_1-25_appetite_scale.docx) regularly to ensure effective risk management development, practice and policy compliance.

## 2.3 ROLES AND RESPONSIBILITIES

The following roles and responsibilities enable the effective application of risk management throughout the University.

### Role of the Court

The Court has a fundamental role to play in the management of risk. Its role is to:

1. Set the tone and influence the culture of risk management within the institution. This includes determining what types of risk are acceptable and which are not, and to provide a framework within which the appropriate level of exposure to risk can be determined in particular circumstances;
2. Approve major decisions affecting the University’s risk profile or exposure.
3. Submit an annual Corporate Governance statement to the Funding Council following advice from the Audit Committee, Risk Management Committee, senior management, external and internal audit.

### Role of the University Executive (UE)

UE is responsible for:

1. Implementing the Court’s risk management policy.
2. Ensuring that the major risks associated with significant proposals put to it have been properly considered and can be appropriately managed within the policy framework and risk appetite set by the Court.
3. Ensuring that corporate risks are properly managed, reviewing evidence to this effect and ensuring measurement of results as appropriate.
4. Communicating University policy and information about the risk management programme to all staff, subsidiary organisations and external partners.

###

### Roles of Heads of Colleges, Schools and Professional Services

Responsibility for identifying and managing the risks in the University, as in any other organisation, lies with the management of the University. Heads of Colleges, Schools, and Professional Services are responsible for:

1. Appointing a senior manager to coordinate risk management within their organization.
2. Ensuring compliance with University and College policies.
3. Identify, evaluate and manage strategic and operational risks and bring emerging corporate risks to UE’s attention.
4. These managers should ensure that everyone in their area of responsibility understands their risk management responsibilities and must make clear the extent to which staff are empowered to take risks.

### Role of the Risk Management Committee

The role of the Risk Management Committee is to support and advise the Audit and Risk Committee, and through it the Court, on the implementation and monitoring of the risk management policy. Its remit is to:

1. Ensure that the identification and evaluation of key risks that threaten achievement of the University’s objectives is carried out, and that a register of these risks is maintained.
2. Identify the strategy in place to manage such risks, including identification of appropriate risk owners, and monitoring the satisfactory operation of the management strategy.
3. Satisfy itself that other risks are being actively managed, with the appropriate strategies in place and working effectively.
4. Report regularly to the Court through the UE and the Audit and Risk Committee on the achievement of the remit. Contribute to raising awareness of risk generally across the University and to maintaining the profile of risk management.
5. Address such other matters related to risk as may arise from time to time.

### The University Risk Manager

The risk manager is a part of Corporate Services Group. They are responsible to the Risk Management Committee for:

1. Facilitating the implementation of the standard risk management framework and process across the University.
2. Assisting with the analysis of operational level risk and the roll-up of significant risks to the strategic level.
3. Providing risk management advice and assistance to all organizations within the university.

### Role of Internal Audit

Internal Audit is responsible for independently and regularly reviewing the operation of the overall risk management process in the University. In doing this, it has regard to best practice as recommended by professional institutes and other relevant organisations. Internal Audit will:

1. Report its findings to the Audit and Risk Committee.
2. Advise and make recommendations to the Risk Management Committee and senior managers as appropriate.

### Role of the Audit and Risk Committee

The Audit and Risk Committee is responsible for monitoring the performance and activities of the Risk Management Committee and reporting there on to Court and in particular:

* + - * 1. To advise Court on the adequacy and effectiveness of policies and procedures for risk management;
				2. To annually review the University’s approach to risk management and, if appropriate, recommend changes or improvements to key elements of its processes, policies and procedures;
				3. To provide an annual statement to the Court in relation to effective risk management; and
				4. Is responsible for the oversight of the assessment of strategic risks that threaten achievement of the University’s objectives, reviewing the University Risk Register and presenting the Register to Court for approval.

### Role of all Faculty and Staff

All faculty and staff have a critical role to play in risk management. As a minimum, all members of the University have a responsibility to:

1. Effectively manage risk within their areas of responsibility in accordance with the University’s risk management policy and process.
2. Report to their superiors risks having wider potential impact, requiring broader coordination, or which are beyond the scope their authority or resources to manage.

## 2.4 ADDITIONAL INFORMATION

To support the University, and to provide risk management advice from a university-wide perspective, the University Risk Manager can coordinate consultation services in areas as diverse as security and loss prevention, insurance, procurement, project management, health and safety, and claims and litigation. For more information, or to engage the services of the University Risk Manager, contact chris.maclean@ed.ac.uk .

[***BS/ISO 31000: 2018 Risk Management –Guidelines***](https://bsol-bsigroup-com.ezproxy.is.ed.ac.uk/Bibliographic/BibliographicInfoData/000000000030315447)

[***Risk Policy and Risk Appetite Statement***](https://www.ed.ac.uk/unpublished/corporate-services/risk-management/risk-management-information)

[***4Risk risk management system***](https://uoeriskmanagement.insight4grc.com/Risk/Home.aspx)

# SECTION 3 **–** APPLICATION OF RISK MANAGEMENT PROCESS

## 3.1 GENERAL

BS//ISO 31000:2018 (*the Standard*) is developed and published by the International Standards Association (ISO), and was adopted by the British Standards Institution as the United Kingdom’s accepted best practice for the implementation of risk management. The University has adopted the Standard to establish the risk management process applied across the institution. It is not a compliance standard, and does not convey any level of certification; it is meant to guide best practice. As a result, the University’s risk management policy and process may differ slightly to accommodate the unique context within which we operate.

The risk management process, illustrated below, is scalable. This means it is just as applicable to the assessment of risks at the strategic University level as it is to small-unit business planning, project management and daily business decisions. Two elements – *Communicate and Consult*, and *Monitor and Review*, occur continually throughout the process. The remainder are usually undertaken sequentially.

Establish the Context

Monitor and Review

Treat Risks

Evaluate Risks

Analyse Risks

Identify Risks

Communicate and Consult

Risk Assessment

Risk Assessment

Adapted from BS/ISO 31000:2018.

Aim to integrate this risk management process into existing business processes, rather than simply layer on another process layer. Clarify goals and objectives, then identify what might stand in the way, and opportunities to exceed expectations. Starting with the strategic goals and objectives of the University, carrying on to Colleges’ and Groups’ service and business plans, through branch and work unit planning, risks can be assessed and mitigated to achieve specific personal, project or program objectives, and ensure alignment with overall University priorities.

##

## 3.2 COMMUNICATE AND CONSULT

*“Communication and consultation with internal and external stakeholders should take place during all stages of the risk management process” (BS/ISO 31000:2018, p.9)*

The consultative team approach means that the assessment of risk is proactive and includes those who understand the risks and are best able to manage them. Often, these people come from those actually performing the associated tasks: data entry clerks, customer service representatives, and administrative assistants, and you exclude their input at your peril. Communicate and consult to ensure that risk reporting goes up to higher levels, but also that executive decisions regarding tolerance of risk and priorities for action get communicated back down to the business unit. Communication is a two-way street.

When conducting the risk assessment, determine the correct balance of participation. It is not always practical or productive to bring all stakeholders to the table. Seek a full range of perspective – advocates and critics, systems, budget, policy, senior leaders, front line delivery and so forth.

Wider participation brings the benefits of greater expertise, experience and buy-in balanced against the requirements for confidentiality, timely action, and strategic scope. The University risk manager can provide advice when deciding which stakeholders should be included in a risk assessment.

## 3.3 ESTABLISH THE CONTEXT

“Establishing the context” for a risk assessment performs a number of functions. Most importantly, it confirms the goals and objectives at risk, identifies stakeholders, and acknowledges constraints and limitations imposed on the organization .

Factors influencing context may be internal, such as executive direction, policies, budget, deadlines and culture; or external, such as government, national or international economic forces, climate and natural events, or citizens and special interests.Establishing the context allows you to:

*… customize the risk management process, enabling effective risk assessment and appropriate risk treatment. Scope, context and criteria involve defining the scope of the process, and understanding the external and internal context.” (BS/ISO 31000:2018, p. 10).*

When applying the risk management process to day-to-day decision making, it may be sufficient to establish the context informally; ask yourself, “How might I best structure this meeting to avoid conflict over some contentious agenda items?” Formal risk assessments, however, benefit from a formal examination and recording of context. A written document will ensure all stakeholders involved in the process have a clear understanding of the context. It also proves invaluable for recording the environment in which the risk management decisions are made, and can demonstrate due diligence if those decisions are revisited later. For this reason, establish the risk assessment’s scope, criteria, and deliverable in writing using the following six headings as a guide:

***1. Subject of the risk analysis:*** What is being reviewed e.g. is it a strategic plan, service plan, project, program, policy, process or procedure? Are you to determine the viability of an idea or concept, or has a decision been made that needs to be implemented? State the scope with respect to organization, hierarchical level, and time frame. Specify whether the context is strategic or operational.

*Hint: If there is no plan or policy yet created, and there is a need for a risk profile on a particular issue, use the status quo as the subject, i.e. the organization’s current approach to the issue. If general goals or values are stated, (see next) the team can generate a risk profile.*

***2. Goals and objectives*:** You should clearly establish what the risk assessment seeks to do because there may be multiple sets of related goals and objectives:

* Those of the University. Clearly establishing strategic goals and objectives will help ensure the subject of the risk assessment is aligned with strategic direction. 4Risk allows you to select from [*Strategy 2030’s*](https://www.ed.ac.uk/about/strategy-2030) ‘[Areas of Focus](https://www.ed.ac.uk/about/strategy-2030/our-focus)’ or ‘[Criteria for Success](https://www.ed.ac.uk/about/strategy-2030/our-university-in-2030)’ the strategic goal/objective that most closely aligns with the risk;
* Those of the College, School or branch sponsoring the program, policy or plan in question. These goals, objectives and major priorities are typically identified in your annual planning submission, and can be uploaded to the 4Risk system to allow each risk to be identified with an objective. The list of goals, objectives and strategies (activities) can serve to structure the discussion of risk.
* Those of the program, project, policy or plan under which the subject falls. These are often identified within the governance documents of major programs, or within standard project management documents like the Project Charter and Project Plan.
* Those of the risk assessment process itself. A risk assessment may inform whether a proposal or project should proceed, or be used to ensure success upon announcement of proposed implementation.

*Hint: If there is no program of activities designed yet, state the highest overall goals, and sketch the main components of a draft plan. This will provide a basis to generate a risk profile and mitigations to inform a final plan*

3. ***Value criteria:*** These are the guiding principles of the organization, such as a professional ethical code, business practices, political priorities, or operating principles found in existing vision and mission statements. They might take the form of special rules; e.g., how to conduct business in a specific context. Participants refer to value criteria in order to help to identify and assess risks.

*Hint: Keep value criteria in plain view during the session. They serve as a common point of reference to help resolve disagreements, and formulate and assess risks.*

4. **S*takeholder analysis:*** This involves the identification of internal and external stakeholders and their respective roles, degree of influence, interests and motives and position with respect to value criteria. They can be both bearers of risk, and/or sources of it.

*Hint: Aim for diversity of participants, (where appropriate and within the limits of the process). This lends both rigour and credibility to the process and leads to a better result. Stakeholder groups who perceive themselves as impacted by a plan can derail efforts when they feel they have not been consulted. Tools to assist in the conduct of a stakeholder analysis are available from the University’s risk manager.*

5. ***Assumptions and constraints:*** Identify deadlines, laws, regulations, policies, resources or other limiting conditions.

*Hint: Legislation, regulation and policy are part of the context in which the risk assessment will take place. Not only do they often address the risks identified, but they also guide the implementation of proposed strategies. Budget considerations may constrain potential mitigation strategies, so identify the fiscal reality within which you are operating.*

6. ***Deliverable for the session:*** Clearly identify the intended product of the risk assessment session. A typical deliverable statement might be *“*a comprehensive list of risks, with rankings and summary treatments arrived at by consensus, to inform an improved business plan/policy/program”.

### 3.3.1 Specialized Contexts: Sub-disciplines within Risk Management

Certain perils or exposures call for a *specialized risk analysis* as a *separate exercise*. For example, extreme weather events or flood hazards create risk exposures in almost any context. Those risks belong to a specialized analysis for *emergency and business continuity planning*. Similarly, security risks with respect to physical dangers, facilities, and procedures, require a *security review*, which is an expertise unto itself. These specialized areas bring their own criteria and resources to bear upon the process.

***University’s Risk Management Strategy***

*Hint: The University risk manager can assist with many of these specialized sub-disciplines, and can refer your team to other experts across the University, such as Legal Services, Fire Safety Unit, and Staff and Student Disability Services.*

##

## 3.4 IDENTIFY RISKS

### 3.4.1 Risk Identification Methods:

### Most often, it is helpful to start with a specific goal, objective, priority or milestone and ask, “what (risk event) might prevent us from achieving this?” A Director or Head of School may ask their senior Leadership Team, “what are the top three risks for your priority objectives”, or “what keeps you up at night” in the context of their work. Some basic tools to help in risk identification include surveys, loss histories, process flowcharts, and expert advice within and beyond the organization. Other tools and methods in more technical or specialized contexts might include:

* Brainstorming
* interview/focus group discussion
* root-cause analysis and bowtie diagrams
* audits or physical inspections
* questionnaires, Delphi technique
* history, failure analysis, and loss reports
* table-top and scenario-based exercises
* personal experience or past agency experience
* incident, accident and injury investigations
* strengths, weaknesses, opportunities, threats (SWOT) analysis
* flow charting, system design review, and systems analysis such as LEAN processes

Some Colleges already have staff with past risk management experience. Consult with internal risk management resources, and inform the University’s risk manager of your risk management activities. In their absence, The University risk manager is a trained facilitator and can assist your organization with the risk assessment process.

### 3.4.2 How to State Risks

Stating risk involves considering its three elements: **event**, **causes**, and **impacts**. Think of the fire triangle with fuel, oxygen, and heat or a source of ignition, where removal of one element prevents or extinguishes fire. Similarly identifying risk by its three elements provides us with three options for treating it. By acting on one of the elements, you can affect the risk.

 

?

Prevent

Mitigate

EVENT

CAUSES

IMPACTS

Cool

Remove

Smother

Avoid

Since we define risk as “*the effect of uncertainty on objectives*” (BS/ISO 31000:2018), start with your organization’s objectives. Define the event as something that could prevent achievement of an objective, milestone or target, or create an opportunity to exceed it. From there, the causes and impacts become easier to identify. Use of a bowtie diagram, as illustrated, can be helpful in identifying multiple causes and impacts of a single event.

***Objective: safety of people in and around the University***

Trip and fall incident

Uneven pavement

Poor lighting

Increased foot traffic during festival

Injury to staff,

students or public

Damage to reputation

Legal liability

Event

Causes

Impacts

A generic example of a negative risk tied to Health and Safety at the University. In this case, a strategic organizational objective is *“safety of people in and around the University”*. A risk event that could influence that is *“Trip and fall incident”*. Causes and impacts flow from this event.

1. Identify a risk event related to an in-scope objective. The event is something that might happen that would indicate a failure to achieve, or an impediment to achieving a goal or objective. Do not state general unfavourable conditions, in and of themselves, as risk events. These conditions may contribute to an event and thus be considered as a cause. While we tend to concentrate on identifying negative risk, it is often valuable to consider opportunities as well. Ask your team, “what might go unexpectedly well that we can exploit to our benefit?”

2. List the potential causes of such an event. There are often multiple causes for a given risk event. Ask yourself “why” the event might happen. Use of root cause analysis methods ([such as the *Five Whys* tool](https://en.wikipedia.org/wiki/5_Whys)) can be effective. Tracing multiple causes using this technique may identify a common root cause, such as obsolete equipment or poor life-cycle management, thus contribute to effectively prioritizing allocation of resources.

3. Identify the impacts of the event, should it happen. Ask yourself, “So what if the event were to occur?” Keep asking “so what” to the chain of impacts until all realistically potential impacts are identified.

The Event, Causes and Impacts can then be recorded in 4Risk, rated to allow for prioritization (see 3.5.1 below), and additional control strategies outlined. Tasks can then be assigned to individuals along with action dates, and follow-up reviews. 4Riskis the tool that the University uses to document the risk assessment and manage the risk management process. Use of one standard process allows risks to be expressed similarly, compared across different parts of the University, rolled-up to the higher level when executive needs to be informed or re-prioritization is required, and reported on through the integrated report-generation feature.

### 3.4.3 Existing Controls

Once the risk is clearly identified detailing event, causes and impacts, it is important to identify existing strategies. Ask “what measures are currently in place (if any) to control this risk?” **List only those mitigations that already exist**. Identification of additional Actions Required (if appropriate) happens later, after the group has evaluated the adequacy of existing controls and the significance of the risk.

## 3.5 ANALYZE RISK

### 3.5.1 Risk Rating

Risk analysis is the process of calculating the likelihood of an event and the severity of the impact/consequence if it were to occur, after considering the effect of the current controls in place. The product of these two variables is the *Risk Rating*.

***Likelihood:*** is the chance that the risk event identified will actually occur. When available, statistical data can support estimates of likelihood and severity. In practice, however, often we do not have historical data. Instead, we often rely on the experience of those around the table, therefore, likelihood rarely implies mathematical certainty; more often, it is a subjective estimate. The matrix below provides a starting point when considering Likelihood, but **adjust the period of time over which likelihood is being considered, depending on your context.** For a project, the likelihood of an event occurring over the life of a project might be appropriate. For a College strategic plan, a three or five-year planning cycle might be a more appropriate timeframe to consider. Agree on this before the assessment, perhaps when preparing the context document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Likelihood** | **Rating** | **Criteria** | **Probability** |
| Almost certain | 5 | Will almost certainly happen this fiscal year or during the three-year planning cycle. | 80% to 99% or once a year or more frequently |
| Likely | 4 | More likely to happen than not. It would be surprising if this did not happen. | 61% to 79% or once every 3 yrs |
| Possible | 3 | Just as likely to happen as not. We don't expect it to happen, but there is a good chance. | 40% to 60% or once every 5 yrs |
| Unlikely | 2 | Not anticipated. We won't worry too much about it happening. | 11% to 39% or once every 15 years |
| Almost certain not to happen | 1 | It would be surprising if this happened. There would have to be a combination of unlikely events for it to happen. | 0 to 10% or once every 25 yrs |

***Impact/Consequence:*** is the severity of effect upon goals, objectives, or values. An organization can adjust the consequence criteria appropriate to their lines of business (perhaps quantifiable in monetary terms), and risk appetite. Many organizations develop a “scorecard” with several categories of consequence, such as *financial* or *reputational*.

|  |  |  |
| --- | --- | --- |
| **Consequence** | **Rating** | **Criteria / Examples** |
| Catastrophic | 5 | * Major problem from which there is no recovery.
* May mean an end to the organization as we know it.
* Complete loss of ability to deliver a **critical** program.
 |
| Major | 4 | * Significant damage to University/college/division credibility or integrity.
* Event that requires a major realignment of how service is delivered.
* Significant event which has a long recovery period.
* Failure to deliver a major commitment.
* Major budget overspend or missed delivery deadline
 |
| Moderate | 3 | * Recovery from the event requires cooperation across departments.
* Budget overspends or delivery delays, but generally within contingencies.
* May generate media attention.
 |
| Minor | 2 | * Can be dealt with at a department level but requires Executive notification.
* Delay in funding or change in funding criteria.
* Stakeholder or client would take note.
 |
| Insignificant | 1 | * Can be dealt with internally at the local level with existing resources.
* No escalation of the issue required.
* No media attention.
* No or manageable stakeholder or client interest.
 |

**Note that consequence ratings can vary depending on the level of the organization that is considering the risk.** A catastrophic risk for a project team may mean total project failure. That same risk, when elevated to the College level, may be significant, but not catastrophic. This is fine and appropriate, and will be guided by the tolerance for a particular risk at different levels.

Likelihood and Consequence scores are multiplied to provide an overall Risk Rating Score. 4Risk will do this automatically, and assign a colour code to correspond with the rating. This is useful to gain a quick visual indication of the highest rated risks. **Note that an inherent weakness of this approach is the tendency to under-rate some exceptionally high-consequence / low probability risks** (such as terrorist acts or pandemic influenza) relative to more likely but moderate impact risks such as modest incidents of fraud or minor injury. Use caution when considering the level of due diligence to apply to these very low likelihood but catastrophic impact risks, as a straightforward comparison of risk ratings may not capture their true relative importance.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Rating Matrix** |  |  |  |
|

|  |
| --- |
|  |

 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### 3.5.2 Risk Rating Terms

The terms associated with the ranking of risks vary across the risk management discipline, but those used by the University are defined below.

***Inherent risk:*** involves rating the risk in the hypothetical absence of any existing controls. This can be difficult to quantify, and so **we do not normally ask risk owners to assess Inherent Risk**, and it is deactivated in 4Risk under its current configuration. From an Internal Audit perspective, there is value in assessing risk this way as it can assist in audit planning, and identify whether a risk exposure is currently over or under-controlled; excessive current controls in the presence of low inherent risk may indicate opportunities to streamline procedures and eliminate bureaucratic waste.

***Residual/Current risk:*** involves rating the predicted risk exposure remaining after consideration of existing controls and mitigation/treatment strategies. It is essential to establish a residual/current risk rating because i**t serves as a start point for an informed discussion of acceptable risk with senior decision-makers**. If the residual/current risk rating, after implementation of existing controls, is sufficient to bring comfort and assurance to senior management, you might need only monitor the risk, without introducing further measures. If residual/current risk is too high, however, you should identify Actions Required to bring the risk within appetite.

***Target risk:*** is a prediction of the risk rating assuming successful implementation of the additional actions required. The Target Risk should manage the risk rating down to within risk appetite.

##

## 3.6 EVALUATE RISK: EXISTING CONTROLS, AND RISK APPETITE

Risk evaluation consists of considering the ranked risk in relation to existing controls and the organization’s appetite, and tolerance for the particular risk in question. The purpose is to arrive at a decision as to how to respond to risks – guided by specific value criteria and cost/benefit. There are three considerations when evaluating existing controls.

1. *Characterize, in qualitative terms, the adequacy of existing controls* (i.e., How would you describe the process, policies, devices, practices or other actions already in place that mitigate the risk in question?) Non-existent or Inadequate, Adequate, Robust, Excessive? This will guide your later decision on *Actions Required*. Non-existent or inadequate controls suggest additional actions are required, and these should be identified, along with who is responsible and when these actions are due to be complete. Adequate existing controls may require only monitoring, in which case a method of review, by whom, and when should be provided. Robust existing controls might suggest this is not a risk at all, or you may wish to document the risk only to demonstrate due diligence, and not take further action. Excessive controls may indicate possible inefficiencies or overspending, or the stifling of innovation, so *Actions Required* might be a plan to review current processes with an aim of streamlining.

2. *Risk Appetite* can help determine the adequacy of existing controls and Actions Required. It refers to the amount and type of risk that an organization is willing to pursue or retain. Court has designated categorized 10 types of risk, each with a range of risk rating they deem “within appetite” for the University, as follows:

|  |  |  |
| --- | --- | --- |
|  | < Less acceptable < to take risks | More acceptable > to take risks > |
|  | 0-5Low | 6-10Medium | 12-16High | 18-25Extreme |
| Reputation | < | > |  |  |  |  |  |  |  |  |
| Compliance | < | > |  |  |  |  |  |  |  |  |
| Financial |  |  | < |  | > |  |  |  |  |  |
| Research |  |  |  |  |  | < |  |  |  | > |
| Education & Student Experience |  |  |  |  | < |  |  |  | > |  |
| Knowledge Exchange |  |  |  |  |  | < |  |  |  | > |
| International Development |  |  |  | < |  |  | > |  |  |  |
| Major change activities |  | < |  |  |  | > |  |  |  |  |
| Environment and Social Responsibility |  |  |  |  | < |  |  | > |  |  |
| People and culture |  | < |  |  | > |  |  |  |  |  |

When entering risk information into the University’s 4Risk management system, risk owners have the opportunity to assign it to one of the risk categories above , and in a separate data field to the corresponding risk appetite. Many risks are easily categorized, and the risk appetite set by court can be used to guide how these risks are managed. When residual (current) risk exceeds the range of appetite above, it is likely that either:

* the risk owner should identify further Actions Required that treat the risk and bring it within appetite; or
* executive should be informed and given the opportunity to expressly accept the current risk rating despite it exceeding appetite, or direct that more be done and allocate the resources required.

Some risks have wide-ranging impacts across multiple categories of risk, so are not easily categorized. In these cases, the risk owner may need to fall back to a more subjective assessment of their tolerance for the residual (current) risk rating, or seek guidance from executive on its acceptability. Risk Appetite is only one consideration when deciding whether further *Actions Required* should be applied. Usually, the lower the risk rating the better so if effective controls can be easily and efficiently introduced to manage the risk rating of even a within-appetite risk lower, do so.

For further explanation of the risk appetite categories, definitions and rating ranges, see the [University Risk Management Policy and Risk Appetite Statement](https://www.ed.ac.uk/sites/default/files/atoms/files/risk_policy_and_appetite_-_new_1-25_appetite_scale.docx).

3. Based on your evaluation of existing controls, decide on specific *Actions Required.* There are generally three types of *Actions Required*

* Treat: If the activity giving rise to the risk should proceed, consider prevention strategies that address the Causes of the risk event, and mitigation strategies that lower the severity of the event if it were to occur. You may also avoid a risk altogether, if unacceptable, by not doing the action that gives rise it in the first place (e.g. unacceptable risks associated with a foreign research project can be avoided by not proceeding with the project).
* Monitor: if existing controls are adequate but the environment is subject to change or uncertainty (the evolving nature of data security risks might be an example), we may wish to implement a periodic review, assigning a specific method, responsible person and date.
* Do no more: Occasionally, if the risk is well managed, predictable and the controls are reliable, stable and tested, you may wish to take no further action and not identify any *Actions Required*, but still enter the basic risk information into the 4Risk system. While the main objective of identifying risks is usually to identify and manage additional actions to lower the risk rating, it may be appropriate to identify a risk and existing controls solely to demonstrate due diligence to regulators, partners or funding agencies.

## 3.7 ACTIONS REQUIRED: TREAT RISK

If the current level of risk is unacceptable or acceptable only with further treatment, you should recommend a mitigation strategy. These are identified in 4Risk as *Actions Required,* and can typically be described as Risk Avoidance, Prevention Strategies, and Mitigation Strategies:

***Risk Avoidance:*** It may be possible to eliminate a risk event entirely by ceasing the activity associated with the event e.g. the risk associated with the foreign travel to a hazardous location can be eliminated by not going, or reduced by selecting an alternative location. This is not always possible or desirable, but it is worth asking if this activity is something that the University ought to be doing. That does not necessarily mean the activity goes undone; a local council contracting out road maintenance and contractually transferring the associated liabilities can be an effective strategy for avoiding specific risks. **Risk *avoidance* is the elimination of risk by ceasing (or contractually transferring responsibility for) the associated activity, but it often introduces new risks, especially reputation loss, or lost opportunity**.

***Prevention and Mitigation Strategies:*** Other than avoidance, risk treatments work to prevent the event by addressing the causes, or decrease its impacts by mitigating the negative effects and preparing for post-event recovery. Ask the group “what might be done to **prevent** the event from happening”, then ask, “If it were to happen, how can we **mitigate/limit** the damage done and get back to business quickly?” As an example, driving at safe speeds can **prevent** the risk of a vehicle accident, while wearing a seatbelt can **mitigate** the impact should the risk occur.

###

### 3.7.1 Diversity of Risk Treatment

As discussed in section 1, existing legislation, regulation, policies and procedures effectively mitigate many risks. These legal, procedural and administrative controls often effectively reduce most risks associated with routine activities to tolerable levels. **The first risk management consideration should therefore be a review of procedural controls already in place, and remedial action to educate and encourage compliance**. Internal Audit is an excellent resource to assist in assessing compliance with policy.

Should existing controls be inadequate, the subject new, or if the context in which they are applied should change, a risk assessment and consideration of additional treatments may be appropriate. Treatments (risk prevention and mitigation strategies) can consist of virtually any sort of administrative action, as well as the application of specialized disciplines where a separate analysis may be required (e.g. emergency planning, business continuity planning, security planning, health and safety treatments, insurance, financial controls, and human resources management). Grouping risks in categories can help in the design of cost-effective treatments.

### 3.7.2 Ensuring Effective Risk Treatment

The following three items are perhaps the most important to ensuring success:

1. ***Actions required are new measures undertaken to control identified risks***. At times, risk assessment participants fall into familiar thought patterns and merely repeat the list of existing controls, and say there is nothing more to be done. Alternatively, they may say that the implementation of their planned program activities constitutes mitigation of risk. It is just here where the facilitator or risk champion may:

* lead off by asking (either “naïve” or well-informed) questions about possible treatments and stimulate discussion;
* draw attention to the ranking of the risk – if participants are reminded that it is high or extreme, and threatens the viability of the program, they will feel less inclined to leave the matter unattended;
* introduce categories of implementation risk (well-documented, common reasons for program failure) to inform the analysis;
* flag the necessity to study the issue and develop treatments “off-line” or in a separate session;
* raise the possibility of inviting expertise from outside the immediate group.

At a minimum, the action of documenting the risk and bringing it to the attention of a higher authority or other entity constitutes at least some due diligence and a degree of improvement in the management of the risk.

2. ***Document Actions required*.** During the latter part of a risk identification and analysis session, make summary statements of treatments. They might have to be elaborated upon elsewhere, but briefly summarizing them allows the facilitator to cover a maximum amount of material. A measure of due diligence is achieved by recording both the risks *and* how they will be managed.

3. ***Translate treatments into action*.** Suggested *Actions required* (preventions that lower likelihood or mitigations that lower consequence) are subject to cost-benefit analysis. The facilitator must challenge the participants to commit to acting upon recommended strategies. If the risk management initiative is an enhancement to existing processes, then the treatments must become new action items in the list of project tasks or business plan strategies. Assigning an individual by name to the development of a mitigation strategy, identifying a specific deliverable, assigning a due date, and listing required resources all bring value and practicality to the risk assessment, and help transform plans into action. 4Riskis formatted in such a manner, and is an excellent tool for Colleges and Groups initiating the process for the first time.

## 3.8 MONITOR AND REVIEW

### 3.8.1 Monitor: Regular Management of Risk Information

Monitoring has to do with managing your risk information as a regular practice. Risks themselves undergo change and can require revision in terms of their description and ranking. New risks appear, conditions change, and *Actions Required* become *Existing Controls* once they are implemented. Therefore, we recommend a periodic (at least semi-annually) updating of risk information, using the 4Risk management tool – perhaps as a standing agenda item in regular meetings. When used to track the implementation of *Actions Required* and the resultant impact on risk ratings, 4Risk and its custom reporting features becomes a valuable communication tool by informing executive on the progress or lack thereof, and any additional resources required.

### 3.8.2 Review: Historical Risk Information

In a mature practice of risk management, a growing body of information can inform analysis of the risks themselves, their most common sources, their frequency and impacts/costs of actual occurrence, the efficacy of treatments, and the occurrence of unforeseen events. All of this serves to better manage risks and inform planning. Audits, complaints investigations, legal judgements, and retrospective cost/benefit analysis are some sources of historical risk information. Another important supporting process is the Risk Questionnaire. Completed annually by all Colleges and Professional Support Groups, this set of 34 questions solicits feedback on major risk-related incidents and losses such as fraud events, misconduct, accidents, etc. By tracking these events over time the University hopes to assess current controls and ensure adequate policies and processes are in place to minimize negative outcomes.

Another important tool that facilitates the collection and analysis of historical information is the *Accident and Incident Report.* It is an important reporting tool for an injury or loss, or incident with the potential to lead to an injury or loss. It allows for tracking of property losses and “near misses”, identification of trends, and development of treatments. As such, it is one of the most powerful tools available to assist in assessing risk. This report is available online and in downloadable form from the [Health and Safety Department Accident / Incident Reporting website](https://www.ed.ac.uk/health-safety/accident-reporting).

## 3.9 RECORD THE RISK MANAGEMENT PROCESS

Risk Management documentation includes:

• ***Set policies and framework*** for implementing and guiding the ongoing application of the risk management process. These documents set risk management goals and expectations, establish the University’s risk management framework, assign responsibilities and resources, establish executive’s risk tolerances and appetite, and give guidance for organization-specific processes, reporting structures, etc. These documents are found in the [*Risk Management Information* section](https://www.ed.ac.uk/corporate-services/risk-management/risk-management-information) of the Risk and Resilience Team website.

• ***Your organization’s risk assessment documentation***, consists primarily of risk information recorded and managed within 4Risk. The risk event, causes and impacts; Current Controls; Actions required, updates and progress notes; and historical changes made are all managed within the 4Risk system risk registers. While detailed functions within the 4Risk system are beyond the scope of this document, the University Risk Manager can help develop and implement your risk management plans.

**The University Risk Manager provides help interpreting and implementing these guidelines. Contact the University Risk Manager at** **chris.maclean@ed.ac.uk**

# APPENDIX 1 – ENTERPRISE RISK MANAGEMENT CULTURE:

# Getting started

Organizations sometimes struggle with enterprise risk management implementation. It is helpful to begin with the view that effective ERM is an end-state. ERM is the outcome of your commitment rather than a process unto itself. It can involve a significant cultural shift which cannot be imposed by edict alone and which takes time to fully mature. ***It is important to recognize the distinction between risk assessments and enterprise risk management:***

## Start With Your Planning Submission

Annual risk assessments are a policy requirement set by the Court. Notwithstanding the policy obligation, this makes an excellent starting point on the path to ERM maturity. An assessment of the overarching operational risks facing your organization, through a risk assessment of your planning submission, is manageable in scope yet corporate-wide in perspective. You will be asking simply, “What could occur that would stand in the way of successfully achieving the goals and objectives of my organization?”

Keep these processes as simple as possible. Many ‘solutions’ sink under the weight of complex and time-consuming steps where the effort is greater than the return. We find facilitated sessions with working groups to be most effective and efficient at producing high quality value-added risk assessments. A representative and knowledgeable working group (the College Registrar, DoPS and Heads of School is a good start) will understand the organization’s operations, its limitations and constraints, and its operating environment. This group can speak to its culture, infrastructure, policies, processes, programs and its people.

If you are new to the risk management process, [this link](https://www.ed.ac.uk/corporate-services/risk-management/risk-management-information) will provide you with more information on the ISO 31000 Risk Management Standard, the University’s Risk Policy and Risk Appetite Statement, and associated guidelines and templates. The same process applies regardless of the scope or type of risk assessment.

A risk assessment to identify, analyse and prioritize key business risks is a tool to guide the execution of your business plan and inform subsequent work. As you would with your business planning and performance management activities, we suggest semi-annual or quarterly reviews of the risk register to monitor for changes to the risk environment, and to update mitigation activities. This operational risk assessment is a critical first step on the road to a more mature risk focused organizational culture. From here, you can push risk management activities downward through the organization. Representative working groups can assess risks facing schools and projects, programme areas and departments. They can review programs, processes, policies and projects.

|  |  |
| --- | --- |
| **Where risk assessments are:** | **Enterprise risk management is:** |
| Narrowly focussed, considering a single level, program or project | Broad-focussed, considering risks across and through the entire organization |
| A moment in time | Ongoing and continuous |
| A tool to focus resources within a project | A tool to redistribute resources across an organization |
| Shared with immediate team and decision makers | Shared with Executive and senior leadership and informs business planning. |
| Typically operational in focus | Typically strategic in focus |
| Managed on a spreadsheet or simple table | Managed via a database for improved reporting |
| Championed by team or project leads | Championed by Executive and senior leaders |

## FROM OPERATIONAL TO LOCAL RISKS

As you press down through the organization, the information gathered becomes more granular and uncovers distinct causes and impacts. For example, at an *Operational* College or Group level your group may identify the threat of an aging workforce. At a *Local* school, deanery or program level, a team may identify the potential loss of a specific skill set or of an individual with specialized knowledge. To mitigate these risks, at the local program level you may respond by addressing the specific issue through job sharing or other knowledge management activities. At the operational College level, your HR Director may consider this and similar risks from other Schools and formulate a College-wide strategy to prevent further staff attrition and mitigate the impacts. At the enterprise/strategic level, the Court may respond by rolling out a strategic HR plan aimed at University-wide hiring policy and retention management*.*

## ROLLING IT UP

Another step in the maturity spectrum is collation of individual risk assessments. Essentially, you are gathering disparate and separate assessments and using them to complete a comprehensive catalogue of an organization’s strengths and vulnerabilities. This collation and analysis provides a snapshot of the organization, identifying potential causes and impacts, which could stand in the way of successfully meeting goals and objectives. This identification of common causes may help support a business case for a new University-wide system, prioritize resources or defend decisions. Over time, through various iterations and planning cycles, these snapshots form a panorama illustrating change over time and trends and ongoing issues. It should demonstrate the effectiveness of your risk mitigation activities and it should help reduce the frequency and severity of negative events. In a maturing ERM culture, executive and senior leaders provide direction on priorities through a consideration of Court priorities and appetite for different risks.

## ERM ROLES AND FUNCTIONS

There is no prescriptive, one-size-fits-all ERM organizational structure below the operational College/Professional Services Group. These structural decisions depend on the size of the organization, the nature of its risks, its culture and risk appetite and available organizational resources.

There are some essential functional requirements. All ERM regimes need a common repository for risk information (we’ve chosen 4Risk), they require analysis and reporting, and they benefit greatly from a champion with good facilitation skills and ability to help build capacity. These functions could be the aegis of one staff member, a dedicated team, or shared more informally throughout the organization. Moreover, ERM requires direction and active engagement from senior leaders.