

# Enterprise Risk Management (ERM)

GETTING STARTED

# Introduction

## Enterprise Risk Management (ERM):

- What is it?
- Is it complex?
- Is it resource intensive?
- Will it cost me money?
- Are we just ticking a box?
- Will it just create added bureaucracy?

Simply put, ERM is just an approach, method or number of processes used to manage risks and seize opportunities related to the achievement of strategic objectives.

It doesn't have to be complex and this document highlights a number of **key themes, simple steps** and **supporting guidance** to follow to help you get started.

It doesn't need to be resource intensive and the key is to develop an ERM approach which is proportionate to the size and shape of your organisation, simple to follow and kept alive by integrating into existing operational processes so it just becomes business as usual.

If you do it right, it can bring many benefits such as supporting the delivery of strategic objectives, informing decision making, reducing the number of shocks and unwelcome surprises, improving strategic planning, protecting your reputation, providing greater assurance and many more.

## Getting started

Risk is part of everyday life and this is no different at work, but we live in riskier times and the world is changing. We face more complex and interconnected risks, with new and emerging risks on the horizon. You need to fully understand them (and the potential opportunities) so you can manage them in a systematic and structured way to provide the confidence that you are on track to meet your objectives.

ERM can really help and below are a number of underlying key themes that have proved valuable when getting started.

- Support from the top
- Build ERM using incremental steps
- Focus on the key risks (a small number of risks at first)
- Leverage existing resources
- Build on existing risk management activities
- Embed ERM into the organisation
- Provide ongoing ERM updates
- Continuously build and refresh.

The table below links the key themes to simple steps and supporting guidance to help organisation's in developing their initial ERM approach.

Key themes	Simple steps	Supporting guidance
<ul style="list-style-type: none"> <li>Support from the top</li> <li>Build ERM using incremental steps.</li> </ul>	<p>Seek Senior Leadership involvement and buy-in</p>	<ul style="list-style-type: none"> <li>Set an agenda item for the Senior Leadership to discuss ERM and its benefits</li> <li>Agree on high level objectives and expectations with regards to risk management</li> <li>Agree on a high level approach, resources and target date for initial implementation.</li> </ul>
<ul style="list-style-type: none"> <li>Leverage existing resources.</li> </ul>	<p>Identify a Senior Manager to lead and drive ERM</p>	<ul style="list-style-type: none"> <li>Identify a person with the right attributes to act as the ERM Champion, e.g. strong knowledge of the organisation and core strategies, good relationships with other Senior Managers, strong communication and facilitation skills, knowledge of the risks, credibility across the organisation</li> <li>Identify objectives/role profile for the ERM Champion</li> <li>Allocate appropriate resources to support.</li> </ul>
<ul style="list-style-type: none"> <li>Leverage existing resources</li> <li>Build ERM using incremental steps.</li> </ul>	<p>Establish a risk management working group</p>	<ul style="list-style-type: none"> <li>Establish a risk management working group to support the ERM Champion and drive the effort across the organisation (example terms of reference available)</li> <li>Ensure the group is made up of the right people, e.g., senior leaders, key staff managers (a good cross section of individuals)</li> <li>Agree objectives/terms of reference of this group, e.g., build an initial ERM framework/approach.</li> </ul>
<ul style="list-style-type: none"> <li>Build on existing risk management activities</li> <li>Focus on the key risks.</li> </ul>	<p>Conduct an initial establishment wide risk assessment</p>	<ul style="list-style-type: none"> <li>Focus on identifying your most significant risks (what is keeping senior leaders awake at night?)</li> <li>Look for risks at a strategic level (aligned to your objectives and priorities)</li> <li>Analyse those risks, e.g., cause and consequences to obtain a greater understanding</li> <li>Prioritise those risks on a risk matrix, e.g., impact x likelihood = risk score</li> <li>Look at existing controls in place and agree whether additional action is required to manage the risks to an acceptable level</li> <li>Ensure appropriate monitoring arrangements are in place, e.g., more serious risks will require more frequent monitoring.</li> </ul>

Key themes	Simple steps	Supporting guidance
<ul style="list-style-type: none"> <li>▪ Build on existing risk management activities.</li> </ul>	<p>Document the existing risk management practices</p>	<ul style="list-style-type: none"> <li>▪ Document the risk management approach and any outputs, identifying any strengths and areas for improvement - this will provide a baseline for the organisation as it continues to develop and enhance its ERM.</li> </ul>
<ul style="list-style-type: none"> <li>▪ Embed ERM into the organisation</li> <li>▪ Provide ongoing ERM updates.</li> </ul>	<p>Develop or enhance initial risk reporting</p>	<ul style="list-style-type: none"> <li>▪ Assess adequacy and effectiveness of existing risk reporting (if any)</li> <li>▪ Look at how ERM can integrate with existing arrangements</li> <li>▪ Develop new reporting formats, e.g., risk heat maps, dashboards</li> <li>▪ Develop a process for considering emerging risks (link into organisation's strategic planning approach)</li> <li>▪ Assess effectiveness of new reporting and key stakeholders and revise as appropriate.</li> </ul>
<ul style="list-style-type: none"> <li>▪ Continuously build and refresh</li> <li>▪ Provide ongoing ERM updates.</li> </ul>	<p>Develop the next phase and ongoing communication</p>	<ul style="list-style-type: none"> <li>▪ Conduct an assessment of the outputs of the working group</li> <li>▪ Revisit the current approach and refine based on initial learnings and good practice</li> <li>▪ Identify next steps to further enhance your approach, including resources and support</li> <li>▪ Seek agreement from the Senior Leadership Team in terms of next steps</li> <li>▪ Continue to raise awareness of ERM throughout the organisation</li> <li>▪ Assess progress and benefits of ERM against objectives</li> <li>▪ Provide ongoing communication and updates in regard to ERM developments.</li> </ul>

**The above is based upon the Committee of Sponsoring Organisations of the Treadway Commission (COSO): Embracing Enterprise Risk Management – Practical Approaches for Getting started.**

This guidance is provided for information purposes based on Enterprise Risk Management best practice and is general and educational in nature.

It does not constitute legal advice. You are free to choose whether or not to use it and it should not be considered a substitute for seeking professional help in specific circumstances.

You acknowledge that over time, this guidance may become out of date and may not constitute best market practice.

Accordingly, Ecclesiastical and its subsidiaries shall not be liable for any losses, damages, charges or expenses, whether direct, indirect, or consequential and howsoever arising, that you suffer or incur as a result of or in connection with your use or reliance on the information provided in this guidance except for those which cannot be excluded by law.

Ecclesiastical Insurance Office plc  
2nd Floor  
Block F2  
Eastpoint  
Dublin 3  
D03 T6P8

[www.ecclesiastical.ie](http://www.ecclesiastical.ie)



Ecclesiastical Insurance Office plc is regulated by the Central Bank of Ireland.

Ecclesiastical Insurance Office plc Reg. No. 24869. Registered in England at Benefact House, 2000, Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW, United Kingdom. Registered Branch in Dublin, Ireland. Reg No. 902180. 2nd Floor, Block F2, EastPoint, Dublin 3. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority in the United Kingdom (Firm Reference Number 113848).

Our Enterprise Risk Management (ERM) support is a non-regulated activity providing optional support to you outside of our insurance products.