PROTECHT

GUIDE

Enterprise Risk Management solutions. A buyer's guide.

What an ERM solution is, why your organization needs one, how to convince other stakeholders that you need one, and how to evaluate which one meets your needs.

Executive summary

What Enterprise Risk Management is and why you need it

Organizations worldwide face a more challenging risk environment than ever before while pursuing their objectives: new risks are constantly emerging, existing ones are changing, and regulatory requirements around audit, risk, resilience and compliance are continually evolving. Section 1 of this guide provides an overview of how the environment is changing and how organizations are responding.

Some organizations manage their risks and compliance obligations in silos, rather than looking at the organization as a whole, which may let things slip through the cracks and leave them overexposed. Enterprise risk management looks across the entire enterprise to understand and manage threats to the achievement of those objectives.

Many organizations have traditionally managed their data and processes manually, by using spreadsheets, emails, or even messaging platforms. Others use siloed automated solutions covering different risk areas that are incapable of holistic reporting. It is increasingly clear that these approaches create risks of their own at an operational level.

As a result, there is a widespread move towards automating risk process using Enterprise Risk Management (ERM) solutions to improve data quality, automate processes and manage regulatory change – and most importantly, to enhance the quality and timeliness of reporting to decision-makers, so good decisions can happen faster.

How to engage your organization in ERM

Risk culture means that challenges are managed in an interconnected way – risks, controls, compliance policies, key indicators, audit information and other elements are all interlinked. This makes it possible to demonstrate how investment in risk mitigation or compliance support will deliver the required results, and how to track those results. Section 2 of this guide provides the steps needed to engage your stakeholders in this process.

As ERM is an interconnected process that cuts across the business, building a consensus to invest in an ERM solution is an interconnected one too. In order to build that consensus, you will need to provide key stakeholders with the information they need to understand how ERM investment will allow them to do their jobs and achieve their objectives – demonstrating that you can achieve a return on investment when taking total cost of ownership into account.

How to assess ERM solutions

Once you reach the stage of seeking an ERM solution, you need to evaluate the different offerings from multiple vendors. Section 3 of this guide considers the key areas along which you should run the evaluation, and provides some sample questions that you should consider asking vendors across the following areas:

- Core ERM solutions
- User support
- Essential workflows
- Robust technology
- Actional analytics and reporting
- Expert implementation and thought leadership

Above all, it's important to remember that risk management is a journey. Using a vendor with expertise in risk management methodologies – not just software – can guide you over your implementation, train your team on risk management best practice, and ensure that you get started as quickly as possible while working with you on a roadmap for future use cases.

Contents

01

What ERM is and why you need it.

1 What ERM is and why you need it

Organizations of all sizes are facing more challenges – of greater complexity – than ever before. New risks are constantly emerging while existing ones are changing. At the same time, regulatory requirements around audit, risk and compliance are continually evolving.

To thrive as a business and meet required obligations, many companies are digitizing. According to a recent survey, 72% of risk executives say that capitalizing on digital transformation initiatives is very important to their company.[1] As part of this shift they are finding they need the support a risk management software partner can provide. Technology enables companies to face new challenges in an ongoing, automated and interconnected way, so good decisions can happen faster.

Figure 1: Challenges that an ERM software solution can address

Risk management	Compliance management	Vendor risk management	IT risk management	Operational resilience	Audit management	Health & Safety
Confidence your risks are identified, assessed and mitigated	A cohesive, shared view of compliance to protect your organization from fines, reputational damage and regulatory action.	Streamline your vendor assessment and monitoring processes.	Gain a clear picture of your information security risks and centralize ongoing management	Identify and self-assess your critical services and operations	Solution aligned with ISO 19011 to support all stages of the internal audit function	Empower your organization to identify, investigate and mitigate health and safety risks and incidents
Continually improve your risk management with dynamic, up-to-date insights	Action-oriented insights through dashboards and reports	Quickly identify and communicate vulnerabilities that need attention	Quickly identify and communicate vulnerabilities that need attention	Centralize data across business units for effective testing, oversight and management of resilience	Quickly identify trends to address key or emerging risks, weak controls or business unit problem areas	Dashboards and reports allow you to address health and safety risks and hazards, and ineffective controls.
Drive engagement with your risk owners and contributors to lift your risk culture	Drive better engagement with obligation owners and contributors	Get an integrated view of vendors with data linked to central risk libraries and controls	Comply more easily with multiple IT Risk frameworks like NIST, ISO 27000, PCI DSS.	Pre-designed dashboards and reports leveraging structured data	Drive engagement with stakeholders to ensure the right action is being taken at the right time.	Drive engagement with your employees to establish, maintain and build your culture of safety

1.1 What is the purpose of this Buyers Guide?

This guide is designed to help those who are considering investing in a software solution to support their enterprise risk management (ERM) processes, which includes internal audit, risk management, compliance, resilience, and health and safety – no matter what part of the organization they are from.

The guide also discusses the importance of having the right expertise to implement ERM software, so that the potential for deploying a successful program is maximized. It provides information that others in your company may find useful when considering how technology can help them.

For example, ERM software can:

- Improve the detection and management of risks
- Document detective and preventative controls that can help the organization prevent compliance breaches
- Provide insights that drive actions, including the ability to determine who owns risks and controls, and the ability to easily present to stakeholders
- Allow risk managers to see the interconnection of risk assessment, control testing, actions, and audit findings
- Allow for a consistent use of control and risk libraries/taxonomies across the organization, so everyone has the same view of the risk
- Drive improved regulatory reporting, enhancing those relationships
- Accelerate internal audit processes
- Reduce the time and effort required for the business to complete compliance tasks
- Enhance the quality and timeliness of ERM reporting to decision-makers, so good decisions can happen faster
- Make it easier to nurture and monitor the right kind of risk culture
- Take a more holistic view of risks across the enterprise

1. www.pwc.com/us/en/library/pulse-survey/executive-views-2022/risk-management-leaders.html

Investing in an ERM technology solution is an important undertaking for all involved – it's critical for the company to purchase the right software and implementation services, to meet its needs both today and tomorrow. This buyer's guide aims to support you and your organization on that journey.

"We were operating with fragmented approaches, and different teams were recording issues and incidents. We realized that what we really needed was to bring these fragments together to develop a holistic view and structured processes around risk management."

Global Head of Risk, Fintech

1.2 Today's challenges

Organizations around the globe are struggling with unprecedented uncertainty – from pandemics to international conflict, economic mood swings to supply chain uncertainties. At the same time, industries are engaging with technology and data in new ways. All this creates risk and compliance challenges. Some strategic issues that companies are facing include:

- The complexity of the risk and control environment – Companies are finding that if they manage risks in silos or as projects, this does not provide a complete enough view of the risks presented.
- Need for ongoing monitoring – Organizations are seeing the need to manage risks and monitor controls on an ongoing basis, and to continually improve their risk management processes.
- Viewing ERM data in an interconnected way – Today's risks are often linked to each other. Controls and compliance requirements are often intertwined as well. Organizations need to have a more holistic, strategic view of ERM. At the same time, this view needs to be clear, uncomplicated, and actionable.
- The accelerating pace of regulatory change – Whether it's new sanctions, ESG regulations, operational resilience policies or cybersecurity rules, organizations are struggling to keep up with all of the implementation work that is required.
- Digital transformation across the organization – Many companies are engaging in substantial digital transformation programs in other areas – often as a result of the COVID-19 pandemic. Audit, risk and compliance teams need to stay aligned, by using technology make their processes more efficient and user-friendly.
- Demands for high quality, timely risk and compliance data from stakeholders – A growing recognition of the value of ERM data means it is needed more by the business, senior management and the board than ever before. Personal accountability rules, such as the Senior Manager & Certification Regime (SMCR) in the UK are also driving this demand.
- Growing focus on data governance for risk and compliance data – For example, the Basel Committee included data governance requirements in the new Revisions to the principles for the sound management of operational risk. Regulators across industries want to know where data is coming from, who owns it, how it is being used, and where it is being stored.
- The need to build a strong risk capacity in a world of labor shortages – This increases the pressure to be efficient with what you have, and partner with a vendor who can provide risk management advice and training.

1.3 Why manual and non-integrated approaches are no longer effective

"[Prior to deploying an ERM solution], our ERM infrastructure consisted of Excel spreadsheets, paper forms and email approvals. Risk and Compliance staff spent the majority of their compliance work on data aggregation and entry – and too little time actually improving our risk culture."

Risk Compliance Officer, Investment Firm

In the face of these trends, companies are finding they need to change their approach to managing audit, risk and compliance processes. Traditionally, many organizations chose to manage their data and processes manually, by using spreadsheets, emails, shared document repositories, and sometimes even messaging platforms.

Even for organizations that have taken steps towards automation, the limitations of siloed systems are also becoming clear. If your compliance management system and your workplace health and safety management system are run by separate vendors and can't easily exchange data between one another, you remain in a siloed position where extracting data and manually creating reports in spreadsheets or reporting tools is the only way you can get a holistic risk view.

This can even be the case within systems from a single vendor, typically in cases where the vendor's growth has been through bolt-on acquisitions: not all systems that nominally support multiple use-cases are able to provide a unified, interconnected dashboard view of risk across your organization.

These approaches can create operational risks for your business, including:

- An inability to see ERM data in a joined-up way that allows you to derive actionable insights for the business
- Lack of robust data governance, specifically lack of audit trail of changes and no ability to see what the data looked like at a point in time
- Data lags and errors, reducing trust in decision-making information
- Difficulty adapting to regulatory change, as manual processes need to be reworked in a manual way
- Reduced efficiency in the business due to process and control breakdowns or the need for frequent remediation to prevent issues
- Increased time and effort spent by the business on risk and compliance tasks, often reducing engagement
- Regulators have less faith in manually collated data due to the lack of governance and audit, making your regulatory environment more challenging
- Failure to manage risk and ensure compliance in a proactive way
- Often additional risk loss events and compliance breaches

Barclays and the SEC

In 2022, global bank Barclays discovered a serious compliance breach in its US operations, leading to fines and buy-backs in excess of US$600 million.

The Securities and Exchange Commission (SEC) requires banks to register the dollar amount of exchange traded structured notes it will sell in a year. This dollar amount is called a "shelf registration". If a bank wants to sell more notes than it planned, it has to go through a regulatory process to register the additional sales.

Barclays had previously held well-known seasoned issuer (WKSI) status, a right that allows banks to sell more than the shelf amount without additional filing. However, in 2017, Barclays lost WKSI status. In 2019, the bank sold 73% more notes than it had registered, thereby committing a major breach of SEC compliance.

The internal investigation found that Barclays' internal controls over financial reporting hadn't been updated to reflect the 2017 loss of WKSI status and the associated change in regulatory requirements. The failure to have an up-to-date and holistic risk management system cost the bank significant financial and reputational damage.

1.4 How organizations are maturing

"We're able to provide our committees with up-to-date information, and all of the visuals in terms of the insights and graphs that our ERM solution can provide are really out of this world. It's literally been life-changing for the organization."

Senior Risk Manager, Insurance Company

These strategic and tactical issues are causing organizations to rethink their approach to audit, compliance and risk management. Analysts at IDC anticipate that companies will be spending more than US$15 billion on governance, risk and compliance software solutions by 2025.[2]

For example, compliance is a rapidly evolving area, with technology taking a larger role as organizations realize they need to automate processes and think more strategically about how they meet their regulatory obligations, according to a recent survey[3], 67% of chief compliance officer respondents indicated that their organizations planned to increase the use of automation and technology over the next one-to-three years. Nearly one-third said they would be enhancing their approach to regulatory change management during the same period. To match these ambitions, more than 75% of respondents said they expect their technology budgets to increase over the next three years.

So, while organizations are facing significant challenges at the moment, there are also signs that their approach to managing these challenges is beginning to shift, with a substantial move towards adopting technology solutions to improve data quality, automate processes and manage regulatory change. Organizations are also seeking ERM expertise to work with in implementing a technology solution, to ensure that the transition delivers real value. These are steps towards a more holistic, strategic view of ERM.

---

[2] https://www.idc.com/getdoc.jsp?containerId=prUS48171921

[3] https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2021/10/kpmg-2021-cco-survey.pdf

1.5 What are the barriers?

While there are a great many factors pushing people towards automation of risk management, there are also some remaining challenges and objections that you may encounter. These generally fall within three main areas:

- **Risk culture** – How people act and behave when it comes to risk management. Factors associated with risk culture may include a lack of budget for technology investment, a conservative unwillingness to engage in major transformations, a lack of perceived importance of risk management as a business priority. Addressing these factors requires a focus on identifying key stakeholders and convincing them both of the business benefits of the ERM solution and of the risks of continuing business as usual.

- **People** – Individuals and teams who are against investment in ERM solutions because they fear job loss from automation, control loss from wider use and access, or increased scrutiny. Addressing these factors requires a focus on the positive benefits of the ERM solution both to risk management and general business teams – showing that the impact will be to free up time to generate business benefits and to provide managers with actionable insight.

- **Advisory** – The organization does not have confidence that it has the expertise to evaluate, implement, mature and evolve an ERM program, even if key stakeholders believe that one would be desirable. Addressing these factors requires an understanding of the options available for help with generating business cases, working with risk experts to specify the solution you require, and implement the software and associated process changes to your organization.

1.6 Next steps

The time for your organization to consider implementing an ERM technology platform is now. Organizations like yours face a wide range of risk, compliance and audit challenges in a rapidly evolving operating environment. Managing these areas manually, in silos, is no longer a good way to achieve your organizational objectives.

Implementing an ERM approach, supported by technology and the right implementation team, enables companies to manage these challenges in an automated, interconnected way at both a strategic and a tactical level. Positive outcomes include better decision-making data, improved risk and compliance management, and enhanced regulatory relationships.

Looking ahead, companies with a robust ERM approach are better positioned to thrive in the world today.

02

Engaging your organization in ERM.

2.1 How can ERM help?

Enterprise risk management – ERM – encompasses governance, compliance, operational risk, financial risk, and non-financial risk. ERM is based on interconnectedness – the ability to collate, analyze and view risk at an enterprise level. By embracing this interconnectedness, organizations can understand their risk profile, enhance appropriate risk taking, and improve their decision making at both a strategic and a tactical level.

The escalation of the Russia/Ukraine conflict

The conflict in Ukraine in 2022, beyond its catastrophic impact on businesses in Russia and Ukraine, created a huge set of unexpected risk conditions for companies throughout the world, even well beyond eastern and central Europe.

According to Eugenie Molyneux, Chief Risk Officer for Commercial Insurance at Zurich Insurance Group, "I have frequently been told that the risks I highlight are too bleak and too negative. But even my worst-case scenario regarding the conflict in Ukraine has been exceeded, particularly with the speed of escalation and extent of its global impact".[4]

The effects of the conflict included some obvious and some less obvious outcomes:

- Gas scarcity in European countries directly or indirectly relying on Russian supply
- Global food shortages as Ukraine's wheat production has been directly disrupted and both Ukraine and Russia's export capacity has been restricted
- Inflationary pressures across the global economy, leading to steep interest rate hikes in many countries
- Credit risks after sanctions removed some Russian banks from the global payments system, including to projects and suppliers which were otherwise unconnected to the conflict
- Supply chain interruptions for major projects (for example, London's replacement Hammersmith Bridge has been severely delayed by disruption to Ukraine steel exports)

The conflict highlights the way that risk scenarios are often interconnected and that viewing interdependencies rather than individual siloed risks is vital to understand the overall picture for your organization.

[4] www.zurich.com/en/knowledge/topics/global-risks/risk-and-resilience-in-a-world-redefined

The ability to adapt and respond faster to unforeseen external risks can be better managed with ERM technology and expertise in place. Cloud-based ERM technology means that data and processes can be accessed from anywhere, to meet business-as-usual requirements as well as the added burden of the crisis situation. Regulatory change can be implemented quickly and easily. Data governance remains robust, so timely and accurate information can be readily supplied to senior management and the board for use in rapid decision-making.

It took the global pandemic for operational resilience to hit the radar – but it shouldn't take another crisis for ERM, supported by technology and expertise, to show the value it can deliver. Overall, taking an interconnected ERM approach greatly enhances the ability of organizations to do the following:

Efficiency

- Automation and simplification of data capture and processes
- Massive reduction in effort for reporting
- Boost business efficiency through better decision-making data and reduced down-time
- Manage regulatory change more efficiently by creating or altering automated processes, such as alerts and attestations
- software is an interconnected one too.

Effectiveness

- Use additional capacity for challenge, horizon scanning…
- Embed risk framework as a business enabler
- Gain new insights from data through robust dashboards and reporting
- Quickly recover and prove it to the regulator, through improved data, auditable processes, and faster and more accurate evidence production

Agility

- Enhance the culture by making it faster and easier for the business to engage in ERM processes
- Quickly adapt to changes in regulations, org. structure
- Configure system through self-service as you mature

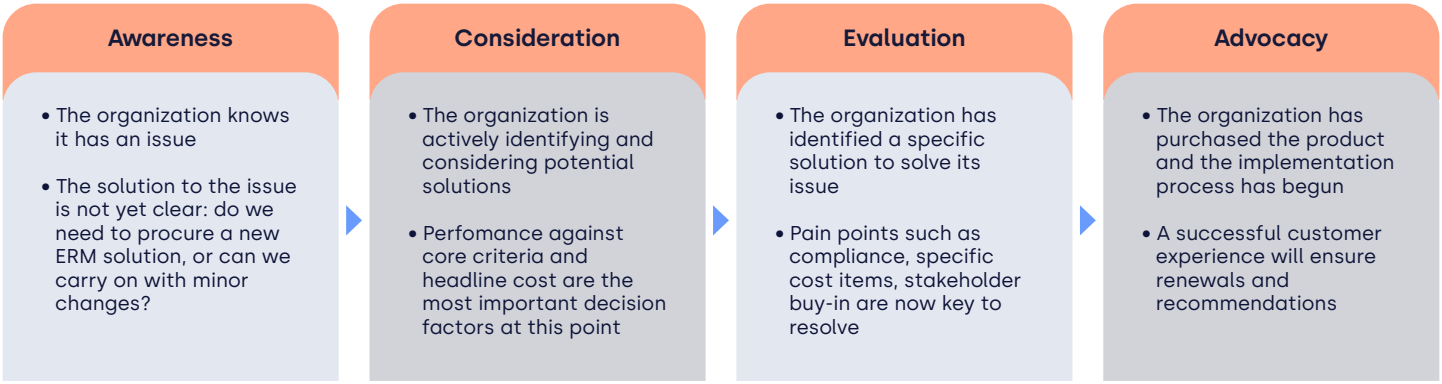
ERM means that all components of risk are managed in an interconnected way – risks, controls, compliance policies, key indicators, audit information and other elements are all inter-linked. For decision-makers, it's clear how investment in risk mitigation or compliance support will deliver the required results, and how to track those results. Overall, ERM supported by the right technology and implementation expertise can help you solve many of the risk and compliance challenges the company faces, enabling it to thrive in today's more challenging ecosystem.

Investing in an ERM solution is a big step for any organization today, and it's important to bring your organization along on the journey. Together, it's important to identify the value that an ERM solution can bring to the organization. ERM is an interconnected process, and it shouldn't be a surprise that building a consensus to purchase software is an interconnected one too.

2.2 What is the buyer journey?

As for any product or service, ERM software solutions follow a buyer journey pattern. If an organization doesn't believe it has any risk management issues, it will be unlikely to embark on the journey. Once it becomes clear that there is something to resolve, however undefined the problem is at this point, then there is a process towards consideration, evaluation, purchasing, onboarding and ultimately advocacy.

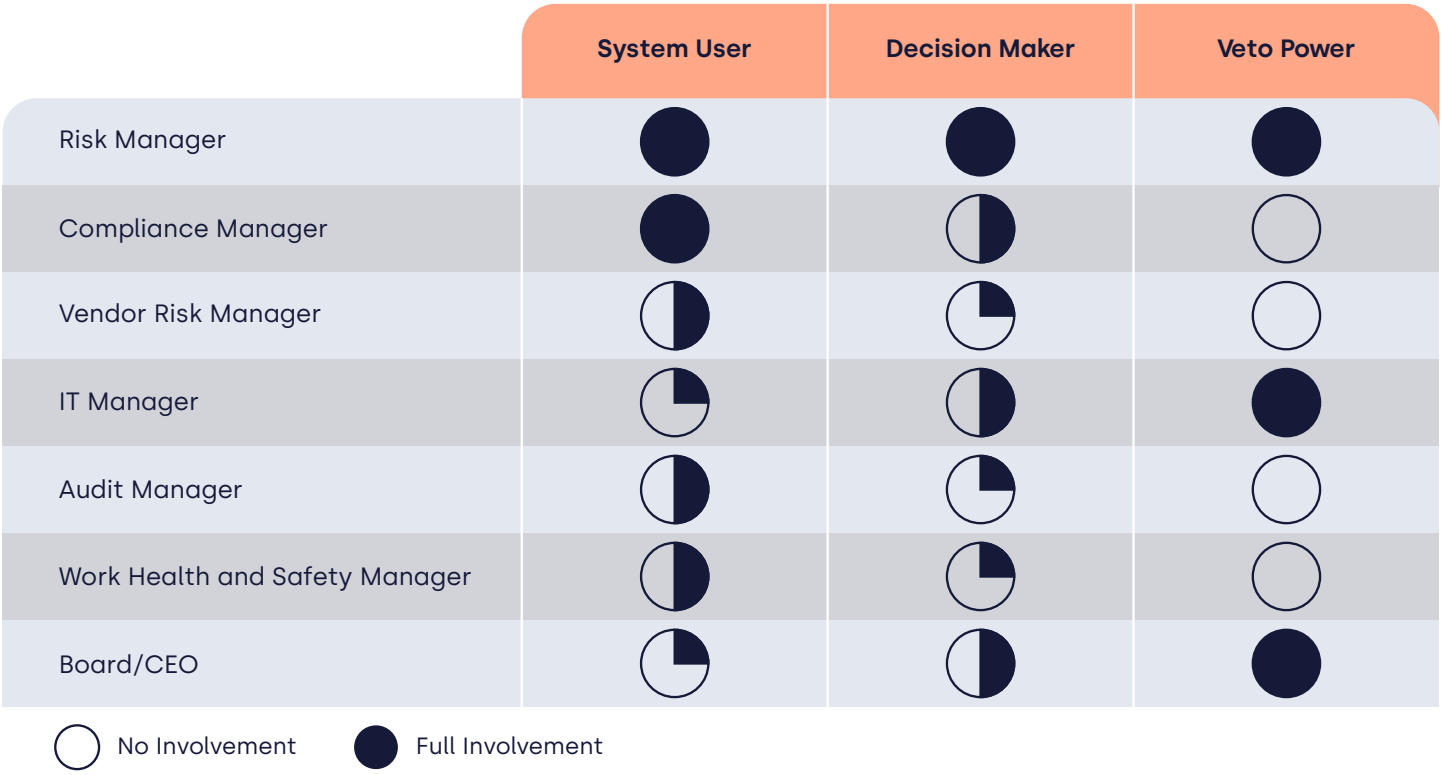
Figure 2: The ERM buying lifecycle



2.3 Gathering information from stakeholders

Once you have recognized the need for your organization to invest in an ERM solution, the first step should be to recognize the other key people who will be involved in the decision-making process and to set up information-gathering meetings. This will enable you to find out their key pain-points and relate this to your requirements for an ERM solution.

Figure 3: Map of stakeholders in the ERM decision-making process



When you are gathering information from stakeholders, you need to follow the following steps:

- Make a list of the key stakeholders in the decision-making process. The list should include both the individuals who have to sign off the purchase, and those who would be influencing a sign-off decision.
- Stakeholders should be from the business, as well as from the audit, risk and compliance teams. If it's possible to engage with senior managers and board directors (such as those on the audit or risk committees), who would benefit from having better data, that is even better.
- Meet with key stakeholders and listen to what those key stakeholders have to say about the audit, risk and compliance challenges that they face every day. Identify the important issues – the ones that most impact the organization. Also look for "low hanging fruit" – the issues that are easily solved by using an ERM solution, for quick wins.
- If you are looking for conversation starters or deeper information on specific ERM topics, look at Section 3 of this document for key questions and answers that we find stakeholders are interested in. The Resources section in Part 4 may also be of interest.
- Acquire data about your current ERM processes. For example, have gaps already been identified in processes? What have regulators said? What are the current levels of risk and compliance breaches? How well are controls working? What are the data governance issues? How confident are senior decision-makers in the data they are receiving? How robust is the organization's ERM culture?
- Ask stakeholders what they would consider important positive outcomes to be from the implementation of an ERM solution – remembering to consider a business rather than a pure risk or software point of view:
  - "I would like to make risk management less painful and more efficient!"
  - "Help me improve my controls!"
  - "I need to be able to feel assured that my team are meeting the requirements that I'm on the hook for under regulatory requirements!"
- All of this can help you build an internal business case now, as well as ensuring that you understand your fellow stakeholders' use cases when you begin to speak to vendors about what you want to get out of your software.

2.4 Building a business case

In most cases, once you have gathered requirements and raised awareness of the potential of ERM within the business, the next step will be to prepare a business case. If your organization has a defined business case template, then obviously ensure that you use it in the expected way. If not, then you can use the bullets below, which should also apply if you are filling out your organization's template:

- Using the information that you have found out from stakeholders, create a clear picture of the important ERM challenges that the organization is facing. Talk about these at both a high level – i.e. managing regulatory change – and at a more detailed level, such as tangible process gaps or issues that have arisen in the past.
- Where possible, collect past event incident and cost data to quantify the challenge. For example, the financial impact of risk events and compliance breaches in a single year, or efficiency losses within a business.
- If possible, quote stakeholders, either named or anonymously, to support discussion of issues that are harder to quantify.
- Explain what ERM is and the role of an ERM technology platform in meeting these challenges and improving outcomes. The resources in Section 1 of this document should be helpful at a macro level regarding risk management – if more information is required, then vendors have a huge amount of relevant material available in white papers, eBooks and webinars. Section 4 contains many examples from Protecht – a good introduction is our Enterprise Risk Management eBook.
- Talk about ERM both at a high level – such as the ability to better manage policy change processes such as attesting to having read a new policy – and at a more tactical level, such as the use of automated reminder emails, automated attestation processes, and reporting to the board as to the success of embedding a particular new policy. As you get into more detail about platform

capabilities, the sample questions in Section 3 of this guide will become increasingly relevant.
- Also discuss, in quantitative terms, the impact that an ERM platform can have on the challenges discussed above. For example, how much time could automating policy management attestations save the business each year? How much time could it save the compliance team?
- Calculate the return on investment in an ERM platform, for example by showing efficiency gains, reduced breaches, improved compliance and regulatory relationships, better decision-making data, and/or enhanced regulatory change management. Online tools can help you determine both the time and the money that your organization could save from an ERM platform, such as Protecht's ERM Return on Investment Calculator.
- Make preliminary contact with a vendor such as Protecht with the above information for a conversation about your needs and how they may be met with a software solution.
- Using the above information, discuss with the vendor how much implementation assistance and training you will need in your organization and include that in your conversation. Make sure you consider not only your organization's implementation and training needs regarding the vendor's specific platform, but also the assistance and training that your organization requires to develop an effective ERM methodology.

2.5 Refine and submit the business case

Once you have created a draft business case and improved your understanding of the benefits and costs of adopting an ERM solution within your business, you can return to conversations with key stakeholders, especially those who are supportive of the project and those who will need to sign off on the purchasing decision.

- It can be a good idea to return to stakeholders positively inclined towards an ERM technology solution with a draft business case to ask them for feedback before submitting it or presenting it.
- It can also be a good idea at this stage to meet with individuals who will be making the purchasing decision, on an informal basis, to discuss the business case for additional feedback, if that is possible.
- Once there is a finalized business case, there may be an internal process that it must go through. Take all the opportunities available to engage face-to-face with the individuals making the decision, to answer questions and address any concerns in advance of the formal decision.
- If the business case is not accepted the first time, ask for feedback so that the business case can be adjusted and resubmitted.

Building a business case properly can take some time, but making this effort will hopefully deliver the benefit of achieving sign-off quickly. It can also ensure you are well prepared for the next stage of the process – speaking to vendors about your requirements, because you will already have much of the information you need to create an RFP at your fingertips.

03

Reference Guide: How to assess ERM solutions.

In this section, we look at the various different ways in which you can evaluate ERM software solutions' performance – both relative to your organization's current baseline and relative to one another. These performance metrics together will determine the return on investment and total cost of ownership of the ERM solution.

We believe that the key areas you need to look at for this evaluation can best be broken down as follows:

- Core ERM solutions
- Supporting users
- Essential workflows
- Robust technology
- Actional analytics and reporting
- Expert implementation

The rest of this section considers key questions that you should consider asking both to yourself and to vendors, segmented by the areas defined above. You should treat this as a reference guide and read through and assess only those questions and solutions which are relevant to your business's ERM evaluation.

3A: Core ERM solutions

In today's organizations, managing risk, compliance, internal audit and other core ERM areas manually leads to complexity, additional risk, and poor-quality data for decision-making. It's important that an ERM solution provides the solutions needed today, and the ability to add on new solutions in the future.

"Our operational teams can report incidents and implement actions in a more timely and standardized manner, our regional teams have fuller oversight of activities, and senior management can take better informed data-driven decisions."

Head of Control and Compliance, Government Agency

Key questions to consider:

- A1: How does the ERM solution support Risk Management?
- A2: How does the ERM solution support Compliance Management?
- A3: How does the ERM solution support Vendor Risk Management?
- A4: How does the ERM solution support IT Risk Management?
- A5: How does the ERM solution support Operational Resilience?
- A6: How does the ERM solution support Audit Management?
- A7: How does the ERM solution support Workplace Health and Safety?

Core ERM solutions	
A1: How does the ERM solution support risk management?	Good ERM software should support the management of risk across the organization in both a holistic and an actionable way. Organizations should be able to use the technology to manage enterprise and operational risks at all levels within the same platform. The full suite of risk management capabilities – such as assessments and incident management – should be available. The solution should also support best practice risk analytics – such as bow tie analysis – dashboards and reporting to enhance communication about risk across the organization.
A2: How does the ERM solution support compliance management?	Organizations ought to be able to manage compliance workflows – including managing regulatory change – within the solution. This can significantly increase efficiency within the company. Organizations should also be able to complete compliance assessments and manage controls within the solution – the software should enable a wide range of controls to be managed. Good compliance and controls analytics ought to allow individuals to see the information that is relevant to them at a glance and keep sensitive information safe through role-based security.
A3: How does the ERM solution support vendor risk management?	A good ERM solution's vendor risk management tools should provide you with a fuller, clearer picture of vendor risk – so you can be confident you're making progress with the right suppliers. The system should allow you to streamline your vendor assessment and monitoring processes. It should allow you to consistently capture key risk management details about the vendors your organization relies on – the relationship, risk assessment, and ongoing monitoring. At a reporting level, the system should provide you with an integrated view of vendors, with data linked to central risk libraries and controls for a holistic picture of how they affect your organization.
A4: How does the ERM solution support IT risk management?	It's important to note that an ERM solution isn't a substitute for integrated cybersecurity software to handle technical areas such as network discovery, network monitoring, vulnerability management, or patch management. From the ERM side, an IT risk management solution works alongside those dedicated tools to give you a clear picture of your enterprise's information security risks, while providing a centralized platform for ongoing risk management. The ways in which an ERM solution can support IT risk management are by improving your asset management and asset risk management, by bringing in a management and assurance policy for IT risk controls, and logging your IT security activities, incidents and policies. At the same time, centralized libraries of risks and controls can allow you to comply more easily with multiple IT risk frameworks like NIST, ISO 27000, PCI DSS.
A5: How does the ERM solution support operational resilience, business continuity management and disaster recovery?	An operational resilience program needs to give you complete visibility over your most critical processes – so you can pinpoint and finetune any potential vulnerabilities along the way. Within your ERM solution, key ways to drive this include end-to-end visibility that allows you to anticipate issues and prioritize resilience; centralized data that allows you to test, oversee and manage resilience across business units. It is also important that an operational resilience solution has been designed from the bottom up to support the regulations and standards that your business needs to meet, and that your vendor has a good understanding of the processes required – whether you're a UK organization who needs to meet FCA and PRA requirements, an Australian customer seeking to meet APRA policy, or an organization in the US or elsewhere seeking to meet ISO 223001 requirements for business continuity management.

Core ERM solutions	
A6: How does the ERM solution support audit management?	A good ERM solution should support the internal audit process, from information gathering through audit report capture and reporting. Alignment with ISO 19011 is a key point to look out for here. Central libraries of risks and controls should be able to be linked to audit findings, enabling the business to better understand the interconnections between those elements. Advanced workflows should mean no more distribution and signing off of reports via email. Live dashboards ought to be able to bring together information so that reporting to risk and audit committees can be streamlined.
A7: How does the ERM solution support environmental/ workplace health and safety?	Having workplace health and safety risks within a dedicated module in an ERM solution enables them to be managed more effectively within the overall risk framework, and at the same time receive the specialized support they need. This module should enable the management of the health and safety of employees and others, such as third-party relationships.

3B: Supporting users

An important part of any ERM solution is that it should incorporate a role-based user experience that is action-orientated, so that specific roles see their domain/perspective of risk that they need to manage and can take action (as opposed to a large data repository that is difficult to gain insights and take actions from). This kind of design also makes it easier to ensure security, confidentiality and data integrity.

Key questions to consider:

- B1: Can the ERM solution be configured to support other use cases?
- B2: Is the ERM solution usable and straightforward for end users?
- B3: Does the ERM solution allow in-house teams to manage user access?

Supporting users	
B1: Can the ERM solution be configured to support other use cases?	With constant regulatory change and emerging best practices, it's important that an ERM solution is configurable for alternative use cases, or specific sub-use cases. For example, the solution ought to be able to be configured to support regulatory change, third party risk management, and other specific solutions that your organization requires.
B2: Is the ERM solution usable and straightforward for end users?	User interface and user experience are hugely important in driving the buy-in among your end users of any enterprise product. Before selecting a solution, it is important to ensure that users are involved – both the risk management team and other key stakeholders should receive interactive demos of the software that make clear its usability and its utility for relevant teams. Vendors can make whatever claims they like for UI and UX, but ultimately the only way to understand if the product is usable for your organization is to try it out.
B3: Does the ERM solution allow in-house teams to manage user access?	Any ERM solution should integrate with your organization's existing single-sign-on protocols to make user access simple and easy to set up. In addition, it should be capable of providing a differentiated solution to make life simpler for end users and ensure your internal administrators are able to control access levels. An effective system should ensure that users are only presented with the fields and sections that are relevant to their roles, and whether these are editable or read-only as appropriate. This functionality should be manageable by internal administrators rather than requiring the vendor to customize the solution.

3C: Essential ERM workflows

Today the range of ERM workflows an organization needs is quite broad, to meet the demands of risk frameworks, compliance obligations, and internal audit requirements – in addition to other ERM use cases. The solution should be able to support the ERM workflow demands of the business, risk, compliance, internal audit, and more.

"We needed a system that was customizable to meet the criteria and terminology within our operational risk management framework, together with a system that allowed for controls testing, incident and issue management and an audit-finding register. In addition, it was important for us to be able to link each key regulatory requirement to the controls in place to mitigate risk of noncompliance."

Senior Risk Manager, Insurance Company

Key questions to consider:

- C1: How are registers created in the ERM solution?
- C2: Do risk & controls libraries or taxonomies help to ensure risks & controls are consistently captured and managed?
- C3: Does the solution support challenges to risk assessments?
- C4: Do Key Indicators capabilities in the solution help to deliver value within an ERM program?
- C5: How does the solution's treatment of obligations content improve compliance management?
- C6: With regulations making accountability important, how does the solution support compliance attestations?

Essential ERM workflows	
C1: How are registers created in the ERM solution?	Different organizations have different needs when it comes to creating registers. A solution ought to offer best practice risk register and reporting templates, designed by risk implementation experts, which are easily accessible for both exploration and use. For start-ups or organizations building their risk controls from scratch, this best-practice templating will help save time and effort in building out a solution. Other organizations – particularly those with established, complex and customized risk management processes – may prefer to re-deploy the paper or electronic forms they already have, and so they should be able to convert these into fully customizable registers using a step-by-step guide. Some organizations will want to design bespoke registers from scratch, and so they should be able to work with implementation experts to design new registers.
C2: Do risk & controls libraries or taxonomies help to ensure risks & controls are consistently captured and managed?	Managed manually or in application silos, risk and control libraries can get out of hand very quickly, with the number of registers growing and the content expanding into long and unmanageable lists. This not only prevents good assessments and reporting, it also results in duplicated effort. For example, the same controls can wind up being used across a range of use cases but described differently in each application. By implementing consistent terminology for risks, controls and causes across the organization within user accessible libraries, organizations can eliminate these issues. A good ERM solution supports this, and then uses this consistency to deliver better reporting and analytics.

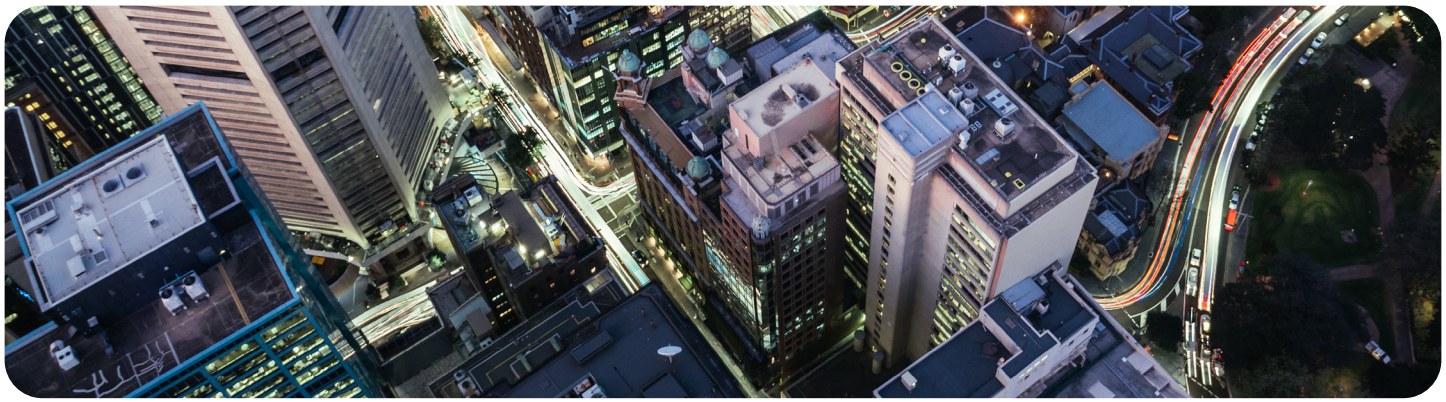
Essential ERM workflows	
C3: Does the solution support challenges to risk assessments?	Risk managers are increasingly interested in being able to challenge risk owners on their risk assessments. Having an analytics tool that allows risk managers to see the interconnection of risk assessment, controls testing, actions, and audit findings allows for more informed challenges. An ERM solution should be able to support these wherever different data points do not tell the story, whether considering residual risk rating assessments, or control assessments that appear incongruent with KRIs. To support these analytics, the solution should enable the organization to create centralized, divisional and group risk assessments as well as control testing to support control effectiveness ratings.
C4: Do Key Indicators capabilities in the solution help to deliver value within an ERM program?	Key indicators – such as key risk indicators (KRIs), key control indicators (KCIs) and key performance indicators (KPIs) – enable organizations to transform their framework into insights and action. Of course, solutions ought to be able to create, capture and manage a range of key indicators. Teams should also be able to input and track key indicators, as well as ensure key indicators can flow into the solution from other systems. The solution should be able to assign the same KRI to multiple business units, and link key indicators to associated items of the risk framework, such as KRIs to Risks. In dashboards and reports, teams ought to be able to see trends in risk appetite adherence and performance metrics.
C5: How does the solution's treatment of obligations content improve compliance management?	Today regulatory change happens at many levels – legislative, regulatory and financial standards, for example. Compliance teams need to understand the jurisdiction, applicability, and impact of rule changes, and then monitor and review changes over time. Having information about changes to regulatory obligations flow within an ERM solution delivers important capabilities to the compliance team. By engaging with embedded regulatory content in plain English – where possible, with automated alerts linked to risks, controls and compliance attestations – compliance teams can action regulatory change demands quickly and efficiently. The solution should notify responsible users when obligations change, and support the impact assessment of those changes. Also, solutions ought to be able to link obligations to incidents, actions, risks, controls, policies, audit findings and compliance attestations so that the compliance program impact is fully understood.
C6: With regulations making accountability important, how does the solution support compliance attestations?	It's important for any ERM software solution today to have a robust and auditable attestation capability. Teams should be able to create automated compliance attestations based on internal or external policies and regulations. Then, they should be able to assign compliance attestations to different users, user profiles and user groups. The software ought to automatically escalate compliance attestations when they become overdue, and force commentary or the provision of evidence when a compliance attestation is outside of policy. Compliance methodologies should support specific regulatory and legal obligations, such as the UK's Senior Managers & Certification Regime (SMCR) for FCA-regulated entities and Australia's impending Financial Accountability Regime legislation, which will extend existing banking sector personal responsibilities to insurance and superannuation sectors. Similar obligations exist in almost all jurisdictions, and it is important to work with a vendor who can confirm their ability to comply with the regimes applying in the countries where you operate.

3D: ERM technology

Having the right technology "in the engine" of an ERM solution is more important than ever before. Data needs to flow seamlessly into and out of the solution, and teams need to be able to access the solution wherever they are working.

"Thanks to the system, a single person with no coding experience, can achieve this in such a short time frame. The support documentation is incredibly well presented, and you can trial new developments in test environments before they are launched. Today, we routinely produce new registers in as little as one day."

Risk Compliance Officer, Investment Management Firm



Key questions to consider:

- D1: What are the solution's data integration capabilities?
- D2: Does the solution support employees who are working from home or are remote working?

ERM technology	
D1: What are the solution's data integration capabilities?	The solution should be able to integrate audit, risk and compliance data from across the organization – pulling from sources such as SAP, Service Now, and more. Ideally, this will also include out-of-the-box integration with external intelligence sources such as LexisNexis or CUBE. The ERM software should be able to send data from the solution to business intelligence applications, such as Power BI, as well as supporting third-party integration platforms. Best practice in most cases is to do this through a fully documented API. In addition to API integration, options such as SCIM and direct file import are a useful additional way of ensuring that users can access the data. It's worth checking with the vendor and your internal support teams whether they have the capacity to integrate their solution with any other proprietary tools you require as part of the implementation process. The solution also needs to be able to be integrated with technology such as Active Directory and Single Sign-On (SSO) technology.
D2: Does the solution support employees who are working from home or are remote working?	The ERM solution should be cloud-based, so that it's possible for employees to access it from wherever they are working, whether on business travel, from home, or from another remote location. At the same time, the ERM software ought to provide iOS and Android Apps that are device agnostic that can provide data capture and review capabilities while online. When in offline mode, these apps should be able to capture data and ensure that this is integrated to the system when the device is next connected to the Internet (e.g. a worker at a remote site using a mobile device to document a safety incident).

3E: Actionable ERM analytics and reporting

Integrated dashboards and rich analytics ought to deliver insights that drive actions. This includes the ability to hold risk and control owners accountable for any actions to be taken, and the ability to easily present to stakeholders – including risk committees, boards and external auditors. When using Excel or disparate systems, this is impossible without using additional software and complex data management/integration. Today, teams working with ERM solutions need to be able to view ready-made visualization dashboards and reports delivering actionable insights that are able to support decision-making by the board, senior management, and the business about ERM.

"Deploying an ERM solution has given senior management the ability to see what is happening within different business functions, and this in turn allows the C-suite to plan for the future using a risk lens."

Chief Risk Officer, Fintech

Key questions to consider:

- E1: What fundamental reporting tools does the solution provide?
- E2: Does the solution include integrated dashboards and rich analytics?
- E3: What kinds of more advanced reporting capabilities should solutions deliver?

Actionable ERM analytics and reporting	
E1: What fundamental reporting tools does the solution provide?	At a basic level, ERM solutions should have built-in reporting that is flexible and which can generate and send reports, from enterprise-wide reports for the board to unit-specific reports for a business unit manager. This should include reports that are generated automatically at specific times or in response to specific events, as well as ad-hoc customized reports. Users should feel confident that data is being handled in the right way, with built-in data security inherited from user roles. The greater the extent to which it is possible to construct the dashboards and analytics that users require within the system, the less need there will be for external exports of data to additional platforms that are no longer covered by your security and audit controls. That said, there will ultimately be a need for any system to provide exports to Excel, PowerPoint, and PDF for external use cases.
E2: Does the solution include integrated dashboards and rich analytics?	Integrated dashboards and rich analytics allow for insights that drive actions, including the ability to assess individual risk and control owners on their performance, and the ability to easily present to stakeholders including risk committees, boards and external auditors. When using disparate systems, this is impossible without using an additional software and complex data management/integration.
E3: What kinds of more advanced reporting capabilities should solutions deliver?	More advanced ERM solutions will have their own complete reporting tools built in, removing the need to export data to other databases and BI tools. Teams should be able to create their own dashboards and reports without coding, using self-service tools. However, if an organization wants to create reporting that is even more sophisticated or is special in nature, it should be able to work with a team of experienced anal ytics consultants to help it design and implement assets for its bespoke requirements. For example, 54% of CCOs said they intend to enhance compliance with subject matter expertise in data analytics, making it the top area.[5] CCOs who need compliance analytics that are bespoke to the challenges that their firm is facing should be able to work with a team of experts to develop the dashboards and reports they need, quickly and efficiently. [5] https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2021/10/kpmg-2021-cco-survey.pdf

3F: Expert implementation and thought leadership

On an organization's ERM journey, purchasing the software is just the beginning. Implementation can seem like it might be long, complex, and expensive – but it doesn't have to be. And in addition to the vendor's implementation capabilities, you need to consider whether they are able to provide accessible risk methodology training, and whether their risk management thought leadership is embedded into the product design and integration.

"The [vendor] advisory staff are a great sounding board for ideas. The advice and guidance we receive on enhancements and updates are very much appreciated."

Enterprise Risk Manager, Fintech

Key questions to consider:

- F1: Does the vendor have subject matter expertise in ERM as well as in the implementation of its own software?
- F2: How easily can the vendor's software be configured?

Expert implementation and thought leadership	
F1: Does the vendor have subject matter expertise in ERM as well as in the implementation of its own software?	Using a vendor that has expertise in risk management as a discipline, as well as in-house expertise for the software implementation, can reduce implementation time and any risk of missed scope or going over budget. The right configurable software allows changes in risk management processes to be implemented quickly and easily without significant cost. Ensuring that the organization's ERM software and processes are aligned is essential to delivering the best results. The right team of implementation experts can ensure that the software reflects the needs of the organization. A vendor that has expertise in ERM should be able to guide the organization throughout the implementation to ensure the new ERM program meets its launch targets. ERM experts can also suggest further areas for program improvement that can be supported by software.
F2: How easily can the vendor's software be configured?	Configurable software allows changes from risk management processes to be implemented quickly and easily without significant cost. Making sure your software and risk processes are aligned ensures greater confidence from stakeholders. Modular cloud-based solutions are generally a better way to ensure this than monolithic locally hosted or desktop apps.

Summary checklist

Organizations seeking to transform their governance, risk and compliance processes – including manual processes – through the use of technology need to consider how well the ERM software and implementation team they are looking to work with supports:

- Core ERM areas
- Essential workflows
- Robust technology
- Actional analytics and reporting
- Expert implementation

By asking key questions, organizations can ensure that they make the right decision about the partner they want to work with to implement a new ERM software platform.

04

Further resources.

Below is a list of just some of the resources that Protecht has created which can help you better understand your organization's risk management needs, as well as specific details of how Protecht.ERM can help you. If you don't see what you need, please get in touch and we will be able to provide documents.

4.1 Enterprise Risk Management Resources

4.1.1 Introduction to ERM	• eBook: Enterprise Risk Management – What does it actually mean to manage risk effectively across the enterprise? • eBook: The Digitization of Risk Management • Webinar: Enterprise Risk Management: Moving from a Siloed to a True Enterprise Approach • Webinar: Risk and Control Self Assessments: How to unlock enterprise value • Webinar: Third Party Risk Management: How protected are you from your third party risks? • Webinar: Risk Appetite – Development and Operationalization • Webinar: Controls Assurance • Webinar: Designing and deploying first rate risk and control taxonomies • Webinar: Using Visual Analytics for Better Risk Management
4.1.2 Culture and Conduct	• eBook: A Definitive Guide to Understanding, Managing and Monitoring Culture Risk, Conduct Risk and Risk Culture • Webinar: Culture and Conduct Risk Management: Bringing it to life with Metrics and Dashboards
4.1.3 Risk Bow Tie Analysis	• eBook: Risk Bow Tie Analysis – The key to analyzing, understanding and managing risk • Webinar: Risk Art Class - Visualize your risk with bow tie analysis • Webinar: Risk Bow Tie Analysis
4.1.4 Compliance	• eBook: The Complete Guide to Compliance and Compliance Risk Management • Webinar: LexisNexis Content in Protecht.ERM – Redefining How You Do Compliance Management • Webinar: Leveraging your ERM Framework to painlessly manage Regulatory and Ethical Compliance
4.1.5 Operational Resilience	• eBook: The Complete Guide to Achieving Operational Resilience • Webinar: Operational Resilience: The ultimate goal in risk management? • White Paper: Operational resilience maturity: How to reach 'sophistication' by 2025

4.2 Risk management digitization case studies

We are always adding new case studies as more organizations join us for their risk management journey. To find the latest examples, visit protechtgroup.com/case-studies

- How WorldRemit uses Protecht to manage risk across 130 countries
- Pinnacle stays in control worldwide with Protecht
- Impax reimagines risk in asset management
- NZ AA: How a mutual organization with 1.8 million members manages risk
- Lotto NZ: Why a lottery operator placed its ERM bets on Protecht
- Freeway harnessing the power of risk in insurance
- How the British Council implemented a centralized audit and incident management system in 100+ countries
- How Melbourne Polytechnic implemented a system that manages risks in a fluid tertiary education environment

4.3 About Protecht.ERM

4.3.1 The Protecht.ERM solution	• eBook: GRC 20/20 Solution Perspective – Protecht.ERM: Redefining Risk Management in an Age of Uncertainty • Webinar: Manage all your risks with an easy to use and configurable system • Webinar Q&A: Protecht.ERM Risk Management System Showcase • Webinar: Protecht.ERM solution Demo APAC -Recording
4.3.2 The Protecht.ERM Marketplace	• Webinar: Introducing Protecht.ERM Marketplace – Optimise your risk management at the click of a button • Blog: 4 Ways Marketplace Will Change Your Enterprise Risk Management

Request a demo of Protecht.ERM today

ABOUT PROTECHT

Redefining the way the world thinks about risk.

While others fear risk, we embrace it. For over 20 years, Protecht has redefined the way people think about risk management. We help companies increase performance and achieve strategic objectives through better understanding, monitoring and management of risk.

We provide a complete solution comprised of world class risk management, compliance, training and advisory services to businesses, regulators and governments across the world.

With our flagship SaaS platform you can dynamically manage all your risks in a single place: risks, compliance, incidents, KRIs, vendor risk, IT and cyber risk, internal audit, operational resilience, BCP, health and safety, and more.

We're with you for your full risk journey. Let's transform the way you understand and manage your risk to create exciting opportunities for growth.

AUSTRALIA & ASIA PACIFIC

+61 2 8005 1265
Level 8
299 Elizabeth St.
Sydney NSW 2000
Australia

EUROPE, THE MIDDLE EAST & AFRICA

+44 (0) 203 978 1360
77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

NORTH AMERICA

+1 (833) 328 5471
Suite 1400
312 Arizona Ave #334
Santa Monica
California 90401
United States

Visit our website:
protechtgroup.com

Email us:
info@protechtgroup.com