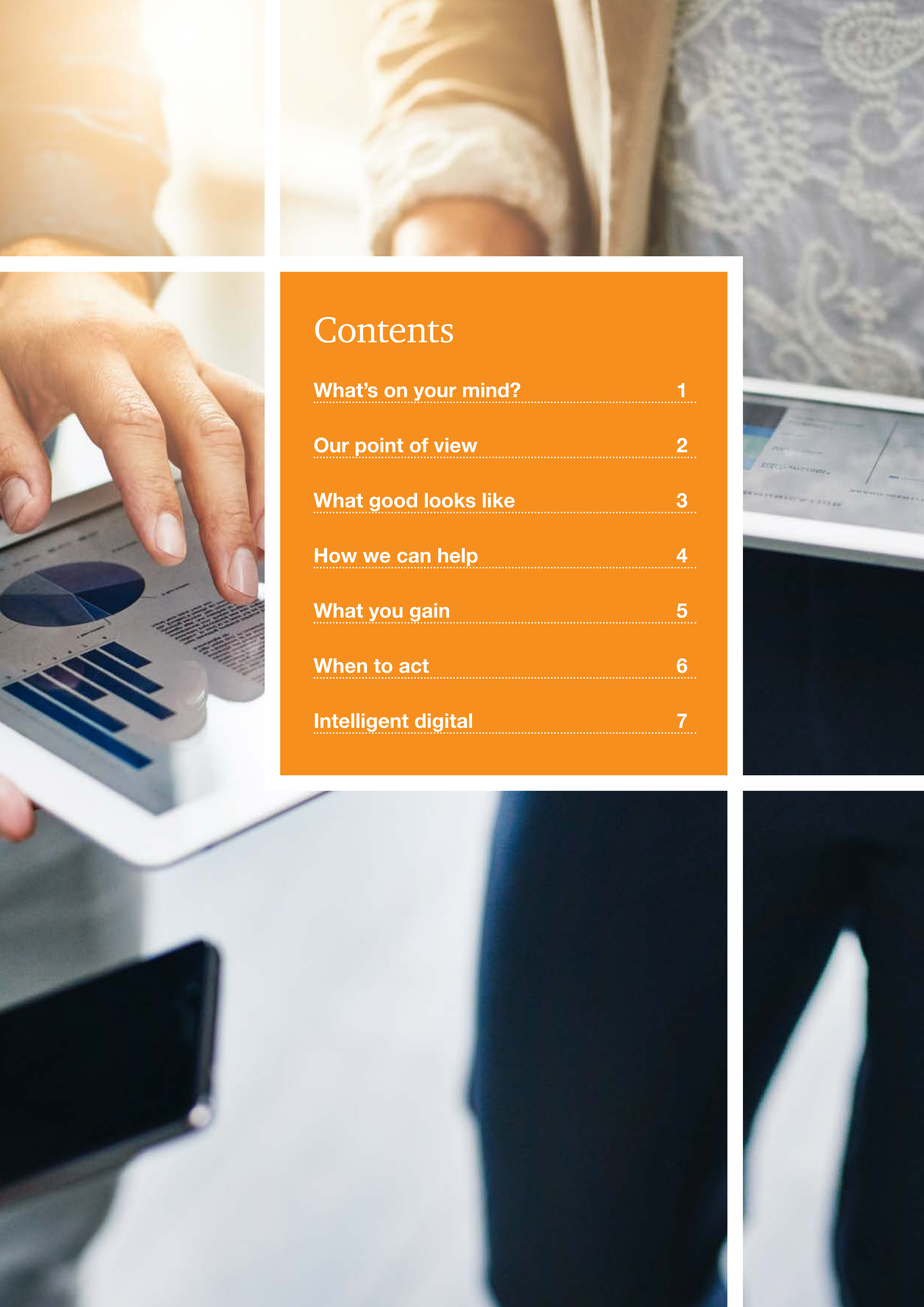
Enterprise Risk Management

pwc



Contents

What's on your mind?

While Enterprise Risk Management (ERM) has existed as a management concept for several decades, many organisations still continue to struggle with deriving full value from their investments in their ERM systems.

Recent updates to international risk management standards, such as the ISO 31000 'Standard on risk management (2018)' and COSO's 2017 'Enterprise Risk Management – Integrated Framework', as well as ongoing developments in corporate governance regimes, have spurred focus by risk practitioners and Boards on the effectiveness and value of their current approaches to risk management.

When discussing these updates with clients, we hear a number of common challenges, questions and comments, from both business users and risk practitioners, including the following:

- The ERM framework does not drive improvements to organisational performance and returns beyond downside risk avoidance.
- The ERM system is overly focused on risk registers and reporting, producing outputs that are static, voluminous and dull, and is completed as a 'tick box' exercise.
- How can I practically articulate risk appetite in a way that will help guide real risk and reward decision-making in the organisation, and help to embed the right risk culture?
- How can I use the data that already exists internal and external to the organisation to better identify and predict emerging changes in the risk environment?
- The strategy/forecasting and risk management processes are not aligned and often disjointed, preventing a full, quantified picture of the potential risks to strategy execution and therefore the capabilities and resources I need to have in place to build and sustain competitive advantage.
- The ERM system does not leverage the power of digital technologies, nor does it help identify and manage the potentially disruptive risks in our industry (e.g. Artificial Intelligence (AI), blockchain and the Internet of Things (IoT)).
- How should risk committees and risk-focused management meetings be structured and run – what is the right governance model, what inputs are needed?

Our point of view

The evolution in risk management and corporate governance standards and codes reflect many of the improvements to practice collectively learned by the risk management community over the past decade. Below is a summary of our perspectives on a sample of common aspects to help you frame your thinking when considering how you can develop more effective and value adding ERM:

- **Adopt a principles-driven view of ERM** – Apply principles of practice that align to the business ways of working and needs, without specifying overly prescriptive or bureaucratic processes, e.g. define minimum standards of quality and rigour, a common language, etc.
- **Get the basics right** – For example, clearly articulated risk descriptions are needed to enable accurate assessment and management response – descriptions that start as 'failure to do something' or there is a 'risk of an objective not being met' can be warning signs of poor risk characterisation.
- **Link risk management with strategy** – A core concept of ERM is to understand risk in the context of achieving strategic objectives. If risk is an afterthought or an alternative risk approach is used in the strategy setting process, this could mean gaps or misalignment. If a risk does not appear to affect an objective or value, what is it?
- **Ensure governance, oversight and management of risk is embedded at all relevant organisational levels** – Are there clear, single points of accountability for each key risk? Is risk management integrated with operational processes, as well as providing top-down perspectives?
- **Leverage and market the use of ERM as an effective communication tool** – Use the organisation's ERM infrastructure and system to provide an integrated platform to communicate identified risks and escalate decisions to senior management, as well as sharing good practice across the organisation.
- **Use data to help ensure the risk system is dynamic** – Risks frequently emerge and change, and the ability to detect and respond quickly can help avoid losses, as well as exploit opportunities. ERM systems based on six-monthly or annual risk register reports that do not leverage available organisational data to power risk indicators often tend to present a more static and limited view of the risk and opportunity landscape.
- **Have more meaningful discussions on risk appetite** – Appetite is not just about preventing high risk exposures and stating what cannot be done, its focus is to support decisions on achieving a consistent balance of target risk and return. **See a further discussion below on page 3**.
- **Address the evolving role of technology in managing risk, as well as it being a source of uncertainty** – Explore the fast-developing capabilities technology offers to strengthen and automate identifying, analysing and responding to risks. **See a further discussion below on page 5**.
- **Question whether you have a productive risk culture** – Are people aware of risk management and the benefits it can provide? Are organisational values, performance incentives and leadership engagement supportive of responsible and desired risk taking behaviours and management?
- **Evaluate your risk reporting** – Explore how current reporting is presented and the content it contains – is it concise, relevant and accessible to the users? **See a further discussion below on page 3**.

What good looks like

Below are three areas of risk management that our clients commonly find challenging, with suggestions on how to address these.

Practical articulation of risk appetite

Risk appetite is a challenge for many organisations, and for some is simply put in the 'too difficult' or 'overly theoretical' bracket. However, when done well, it provides significant benefits in promoting organisational awareness of how risk taking supports strategic execution and the risk envelope in which management levels can operate. Outside of Financial Services, where this concept is well established, we have seen increasing maturity and sophistication in how appetite is articulated, progressing beyond simple statements and 'hungry and averse' scales, to more objective, metric-based outputs linked to performance targets and measured with risk indicators. Useful steps to ensure practical articulation include:

- Discuss with the Board and the Executive Management team which type of risk appetite articulation best fits your organisation – who will use it, when and how?
- Consider risk appetite in the context of strategy, analysing the relationship with both principal risks and those risks (singular and portfolio) that can deliver strong upside and returns (which may not necessarily be 'principal' downside risks).
- Communicate risk appetite in business language, not risk-centric language, using quantifiable metrics wherever possible. For example, the thresholds of KPIs and Key Risk Indicators (KRIs) can serve to communicate, promote and measure risk-taking behaviour at operational levels if their relationships and sensitivities with the risk in focus is analysed and understood.

Addressing the evolving role of technology in managing risk

Evolving technology continues to disrupt industries and the strategic status of many organisations, as well as the discipline of risk management itself. ERM practices and capabilities need to address and inform on both the emerging risk environment and velocity of change, as well as becoming digital in their own right to ensure the discipline exploits more effective and efficient ways of working. To help do so:

- Use 'Emerging Technologies' as a strategic theme to drive discussion with the Board and management on emerging risks and scenarios and how they could either disrupt or beneficially transform the organisation's strategy and operations.
- Consider how technological developments and improvements in data analytics can be used to generate further risk insight to aid in decision-making, e.g. automated risk monitoring, predictive modelling, etc.
- However, also recognise that successful management of risk is driven by the knowledge, experience and engagement of staff: avoid the tendency to view technology as a panacea for effective risk management.

Enhancing risk reporting

Whilst reporting using 'tried and tested' red/amber/green risk lists and heat maps have been useful for many organisations in their formative years of establishing ERM, most soon outgrow these approaches and want something better. This can be due to the volume of reporting that grows over time so recipients struggle to see the static risks that are still included and dilute focus from what really matters. Or perhaps failing to leverage available data to provide dynamic insights to aid decision makers. To help rectify this:

- Develop reporting dashboards and templates with increased use of graphics and diagrams to make it easier for the reader to engage with the information.
- Focus attention on the key areas of risk change/development in the period under scrutiny and the questions or issues that require prioritised management awareness and response. Static information can be added in an appendix if necessary, i.e. focus on exception-based reporting of data in the body of the document.
- Leverage data analytics, modelling and KRIs (where it is useful) to provide predictive and objective views of risk, aligned to risk appetite, so that the focus is not on whether a risk is significant but whether the current exposure level is unacceptable.
- Align risk with performance reporting. For example, when reviewing KPIs, focus reporting on the risks with strong correlations to achieving those KPIs, how severe those risks are, how they are changing over time and what this means for forecast performance.

How we can help

We evaluate, design and implement full-spectrum ERM systems and operating models, to ensure clients can effectively manage risk, aligned to their goals and cultural ways of working. Our approach and methodologies incorporate decades of experience successfully partnering with clients of all shapes and sizes. This allows us to leverage insights, benchmarks and optionality to ensure we deliver ERM systems that are bespoke and work in reality whilst reflecting common good practice and leading approaches.

Our track record of success

A small sample of our engagements include:

- The redesign and implementation of a new ERM system for a major **global extractives firm**. The work considered all elements of an ERM framework, including consistent and robust risk identification, assessment and aggregation techniques, high-impact risk management, risk strategy and appetite, group risk governance, reporting structure and templates, risk assurance and cultural integration and training.
- For a **global investment bank**, we developed their supplier risk management framework using ERM concepts and principles in the design. The work included risk profiling of an extensive third-party estate to identify the most significant exposures, creation of desktop risk assessment and predictive analytics tools and reporting, training of the global procurement community, and development of a low-cost offshore supplier risk assessment service.
- We designed and supported implementation of the ERM system for one of the **UK's largest and most complex public sector bodies**. The project included development of all policies and procedures, critical risk profile analysis, articulation of risk appetite and KRI suites, and ongoing implementation support via training and workshops at all organisational levels.

What you gain

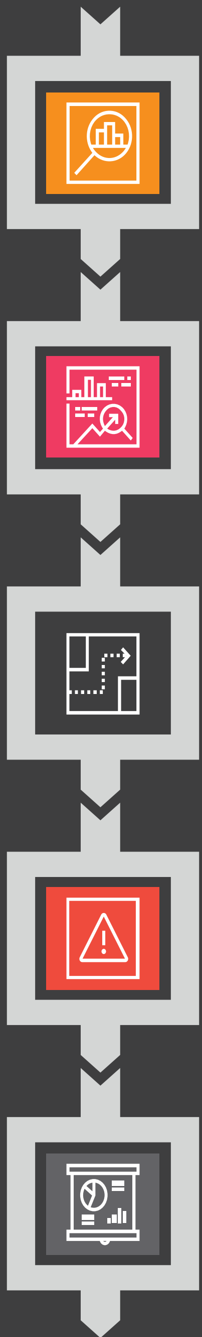
The typical benefits that our clients can expect to realise through engaging PwC to support their ERM development objectives include:

- More informed decision-making and efficiencies in resource allocation.
- Consistent and robust identification, analysis and mitigation of key risks in line with risk appetite.
- Clarity in accountability and ownership of risks.
- Improved view of risk relevant processes and controls, including effectiveness quantification.
- Leverage of existing organisational data to provide predictive views of risk exposure.
- Clear pathways to raise significant risks via escalation and reporting channels that are timely and insightful.
- Development of a proactive, risk-aware culture.
- Enhanced assurance to the Board and Audit/Risk Committee(s).

When to act

Our clients appreciate that ERM plays an important role in their corporate governance concerns and strategic execution, but knowing when to seek support in this area is not always obvious.

From our experience, we recognise a number of common triggers that should prompt organisations to seek out support and advice in ERM:



There are known weaknesses in the current ERM programme. This could be evidenced by actual losses and near misses, or feedback from users that the approach does not add value, poor internal audit review findings, etc.

A competitor has suffered a major loss or exploited a significant uncertain opportunity that is relevant to your organisation.

There is a major change to the organisation's strategy/operational profile/external environment that requires a new ERM approach.

Recent actions, behaviours and/or performance have shown your risk exposure is misaligned with your company's risk appetite.

New and emerging technology, standards and methodologies to manage risk more effectively become available.

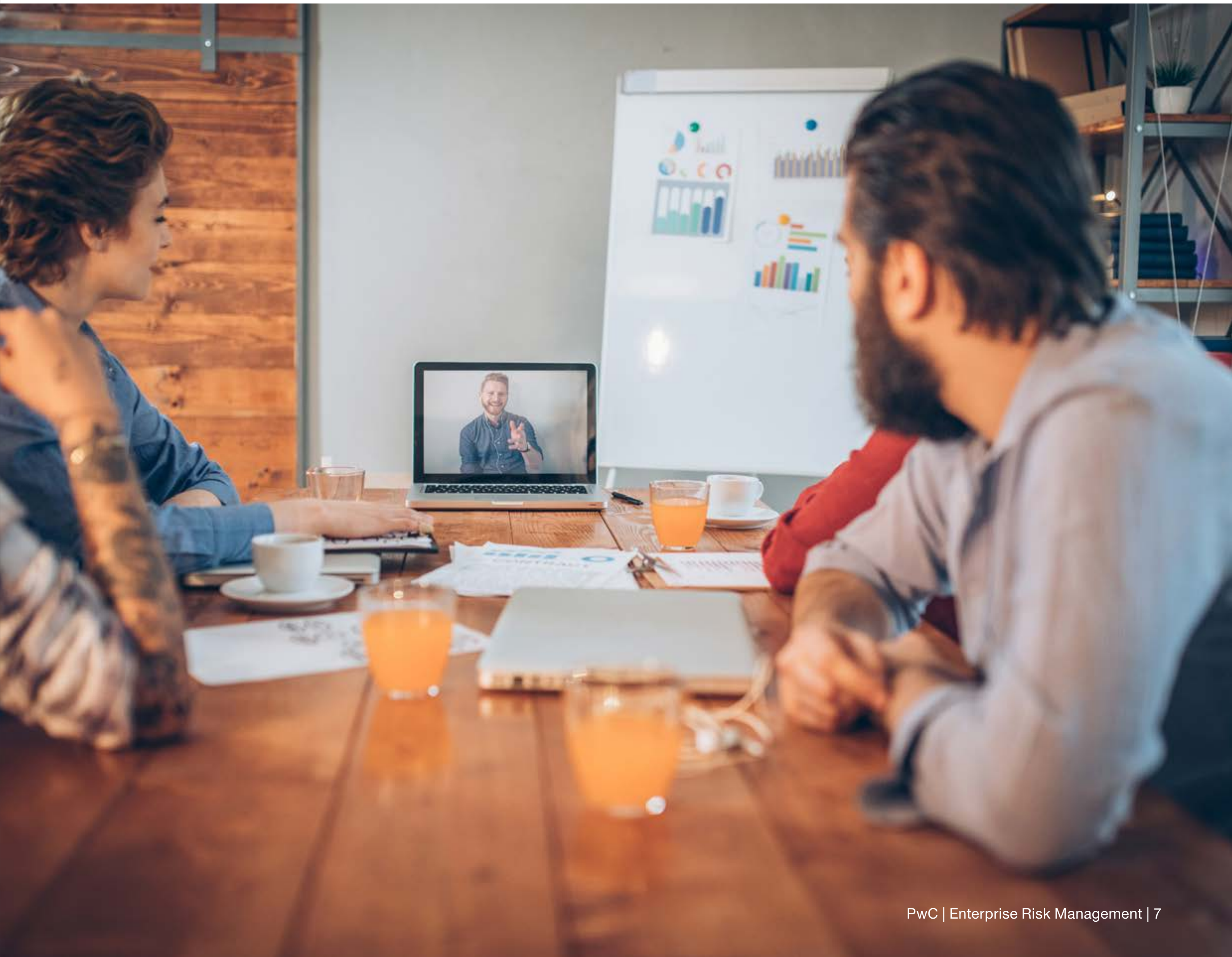
Intelligent Digital

At PwC, we are harnessing the power of Intelligent Digital, helping our clients to rethink their futures and reshape their own world. We are using business understanding, innovation in technology and human insight to help solve important problems, meet human needs and make a difference to society.

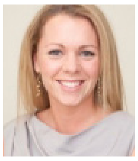
Drawing on data to create in-depth reports around systemic risk is a positive way for organisations to make use of the latest technologies to bolster their ERM activities. At the same time, the evolving nature of the global risk landscape means new tools are being developed all the time to help businesses to better understand their risk exposure.

At PwC, we bring a wealth of experience in managing ERM for our clients across a wide range of industries and locations, supporting them with access to the newest technologies that feed into our Intelligent Digital philosophy.

pwc.co.uk/intelligentdigital
#IntelligentDigital



Get in touch



Hayley-Beth Peters
Director – Enterprise Risk Management Lead, Non-Financial Services,
PwC United Kingdom

M: +44 (0)7740 242402
E: hayley-beth.peters@pwc.com

Richard Bailes
Partner – Governance, Risk and Compliance,
PwC United Kingdom

M: +44 (0)7715 034917
E: richard.j.bailes@pwc.com

Callum Bright
Senior Manager – Enterprise Risk Management, Non-Financial Services,
PwC United Kingdom

M: +44 (0)7802 659019
E: callum.b.bright@pwc.com

2021-08-26_RITM6047161