Business Voice Report Risk Webinar

Using ERM to Balance Risk and Reward

March 2022

With you today

Sara McAllister

Partner, Business Risk Services. Grant Thornton

Sara is a partner in Grant Thornton and Head of Business Risk Services for the Irish firm.

She is a highly accomplished risk professional with over 25 years national and international experience across all aspects of enterprise risk, operational risk and controls assurance.

Sara started her professional services career in a Big 4 firm and has held a number of senior Risk, Compliance and Internal Audit positions both in professional practice and industry at home and abroad.

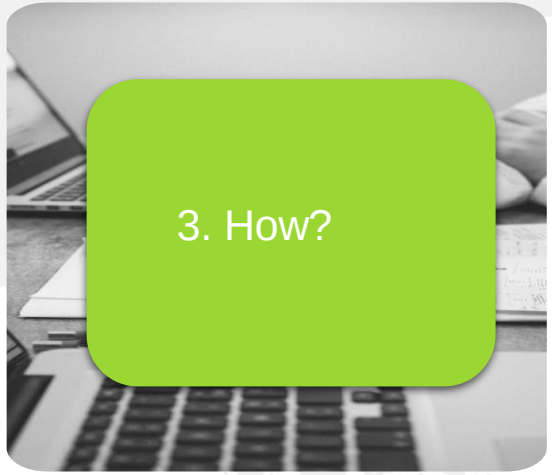
She advises clients across a broad range of sectors including technology, pharmaceuticals, food and beverage, distribution and consumer goods. She is commercially orientated and focuses on providing clients with business insight across governance, risk, security, control and process efficiency challenges.

Sara is a fellow of Chartered Accountants Ireland (ACA) and she holds the following qualifications:

- Postgraduate Diploma (Masters) in Advanced Banking Risk Management, U.C.D
- Postgraduate Diploma (Masters) in Accounting, U.C.D
- Bachelors of Commerce (Undergraduate Degree) , U.C.D
- Six Sigma, Green Belt

Purpose

Today’s presentation will cover an overview of Risk Management:



Enterprise Risk Management

Overview

The primary objective of Enterprise Risk Management is to ensure that the outcomes of risk taking activities are consistent with an organisation's strategic objectives, business plans and risk appetite, and that there is an appropriate balance between risk and reward.

COSO and ISO 31000 are the Risk Management best practice frameworks.

Traditional RM approach Vs ERM

Comparing Traditional Risk Management with ERM

Aspects of a traditional RM Approach

- Silo based (Vertical)
- Incomplete risk coverage
- Lack of standardised approach
- Inadequate reporting
- Unowned risks
- Lack of integration
- Not aligned to performance management

Aspects of Enterprise Risk Management

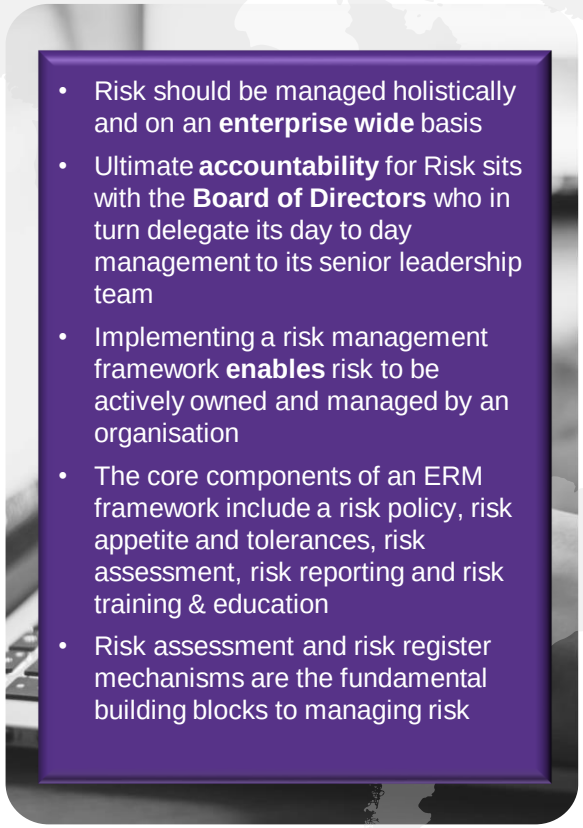
- Holistic (Horizontal)
- Standardised
- Focus on inter-relationships
- Risk is integrated to performance management
- Full risk accountability
- Better resource utilisation

In contrast with the traditional approach, ERM recognises that risks in one part of the organisation can relate to risks occurring elsewhere and these links and relationships need to be managed just as much as individual risks in isolation.

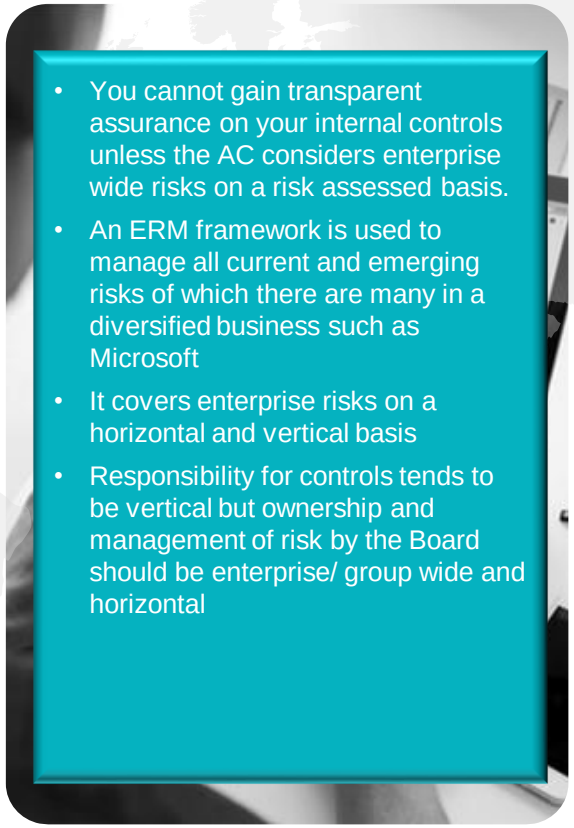
Enterprise Risk Management

Features

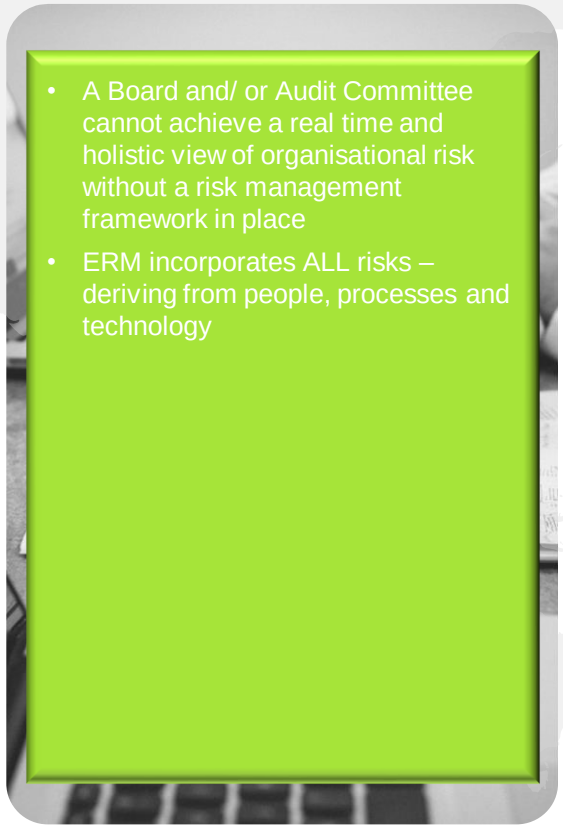
The primary objective of Enterprise Risk Management is to ensure that the outcomes of risk taking activities are consistent with the organisation strategic objectives, business plans and risk appetite, and that there is an appropriate balance between risk and reward



- Risk should be managed holistically and on an **enterprise wide** basis
- Ultimate **accountability** for Risk sits with the **Board of Directors** who in turn delegate its day to day management to its senior leadership team
- Implementing a risk management framework **enables** risk to be actively owned and managed by an organisation
- The core components of an ERM framework include a risk policy, risk appetite and tolerances, risk assessment, risk reporting and risk training & education
- Risk assessment and risk register mechanisms are the fundamental building blocks to managing risk



- You cannot gain transparent assurance on your internal controls unless the AC considers enterprise wide risks on a risk assessed basis.
- An ERM framework is used to manage all current and emerging risks of which there are many in a diversified business such as Microsoft
- It covers enterprise risks on a horizontal and vertical basis
- Responsibility for controls tends to be vertical but ownership and management of risk by the Board should be enterprise/ group wide and horizontal



- A Board and/ or Audit Committee cannot achieve a real time and holistic view of organisational risk without a risk management framework in place
- ERM incorporates ALL risks – deriving from people, processes and technology

Enterprise Risk Management

Benefits of ERM

Meet Strategic Goals

Governance

- Risk management driven from top down and executed from bottom up
- Better communication to and information for the Board / Senior management
- Greater assurance and confidence in control environment
- Faster and better informed strategic decisions

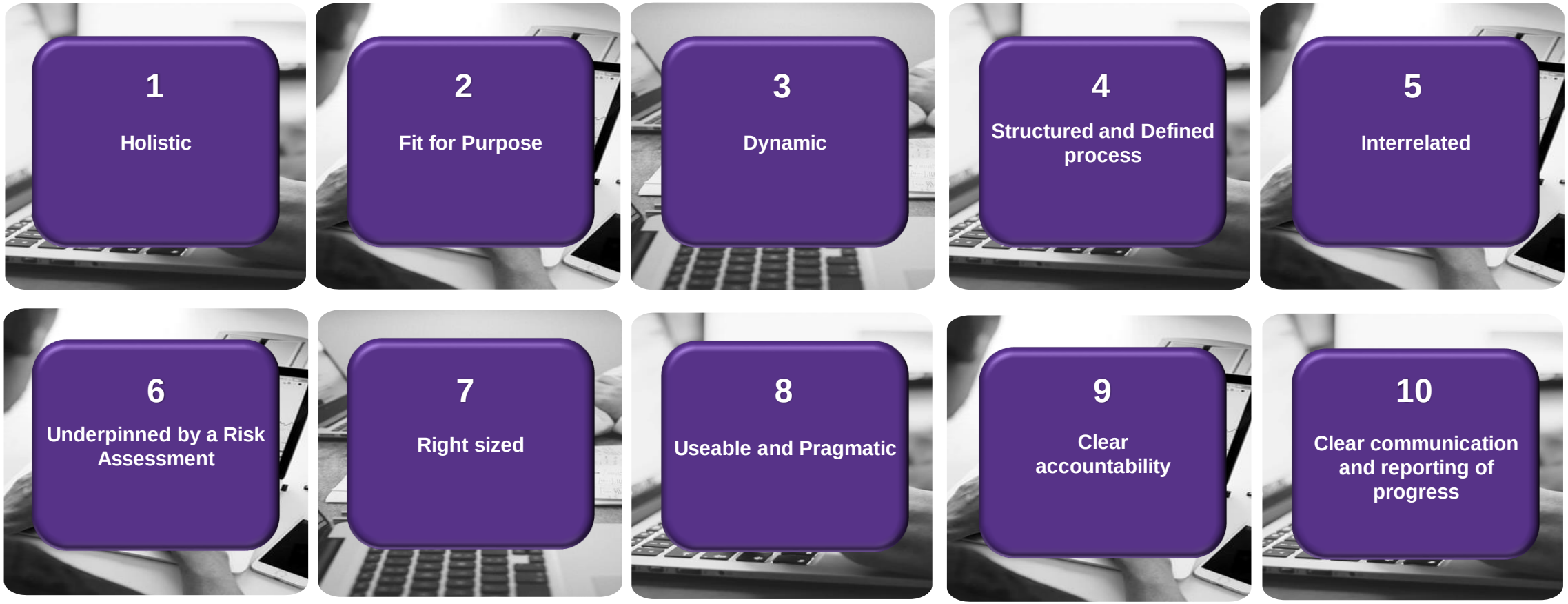
People & Process

- Risk aware culture across the organisation
- Consistent risk practices across business processes
- Compliance, a nurtured but natural and assured side-effect
- Risk/ reward, the key success criteria – improved performance management and accountability/ responsibility for risk management and control health

Business Management

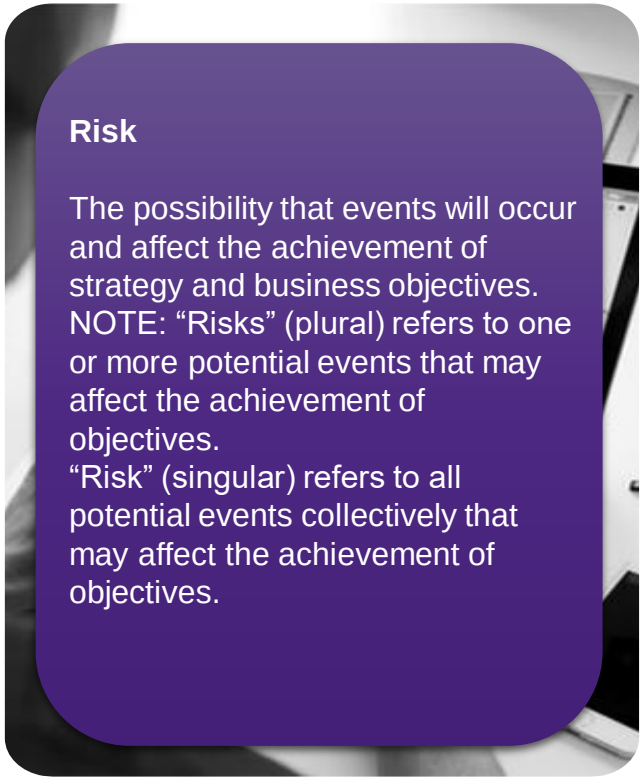
- Business objectives protected and secured
- Risk opportunities identified & knowingly / safely pursued in line with clearly articulated risk appetite
- Risk embedded in all business decisions (strategic and operational)
- More accurate risk pricing of contracts/ services
- Better deployment of capital & resources

Critical Success Factors



Definitions

Risk and Risk Management



Risk

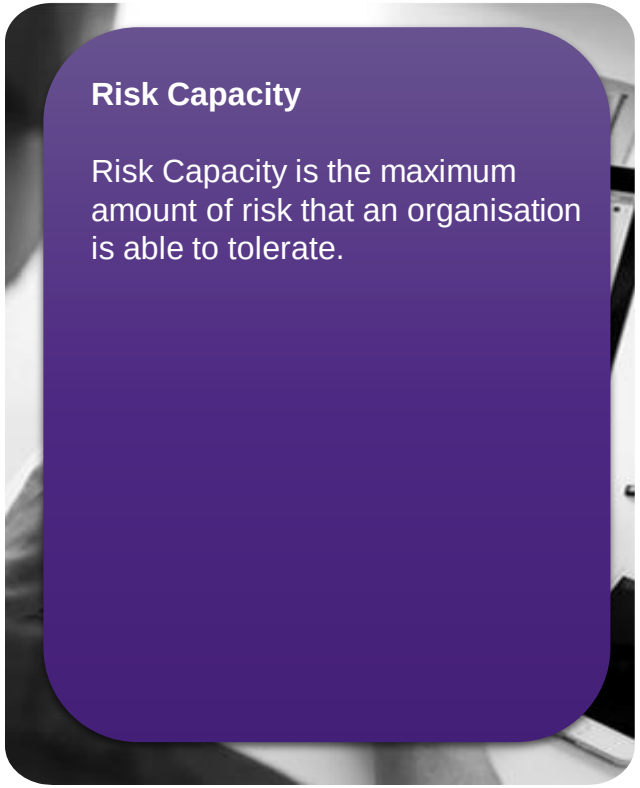
The possibility that events will occur and affect the achievement of strategy and business objectives.
NOTE: “Risks” (plural) refers to one or more potential events that may affect the achievement of objectives.
“Risk” (singular) refers to all potential events collectively that may affect the achievement of objectives.

Risk Management

COSO definition of risk management is – “a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

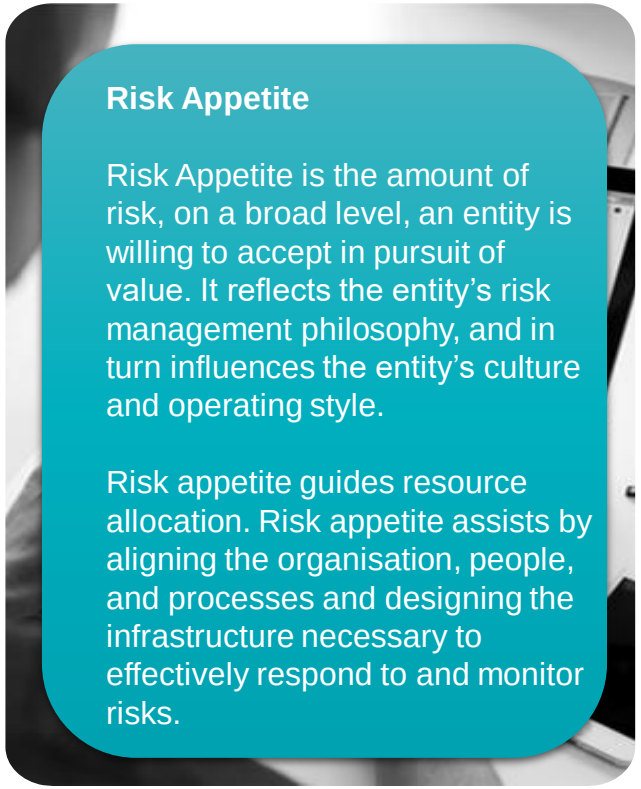
Definitions

Risk Capacity, Risk Appetite and Risk Tolerance



Risk Capacity

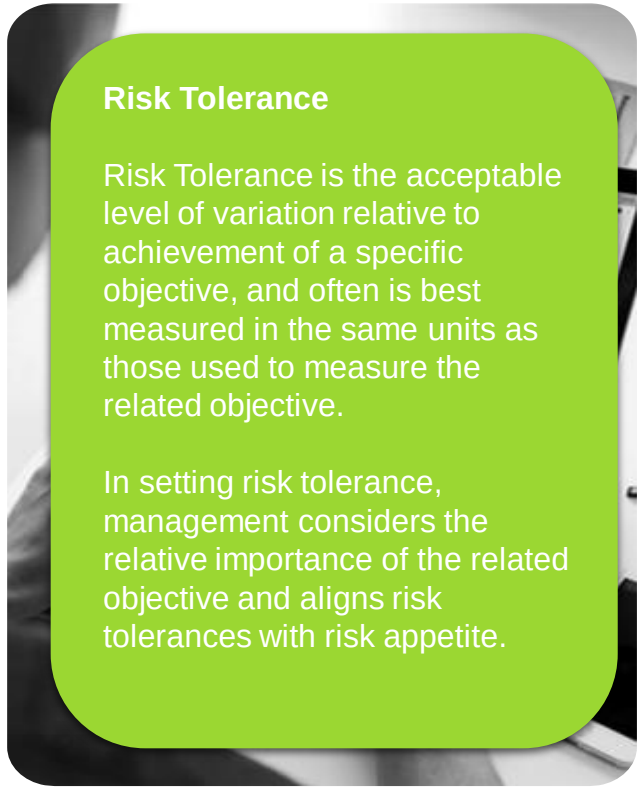
Risk Capacity is the maximum amount of risk that an organisation is able to tolerate.



Risk Appetite

Risk Appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style.

Risk appetite guides resource allocation. Risk appetite assists by aligning the organisation, people, and processes and designing the infrastructure necessary to effectively respond to and monitor risks.



Risk Tolerance

Risk Tolerance is the acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective.

In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite.

Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives.

Enterprise Risk Management

Framework

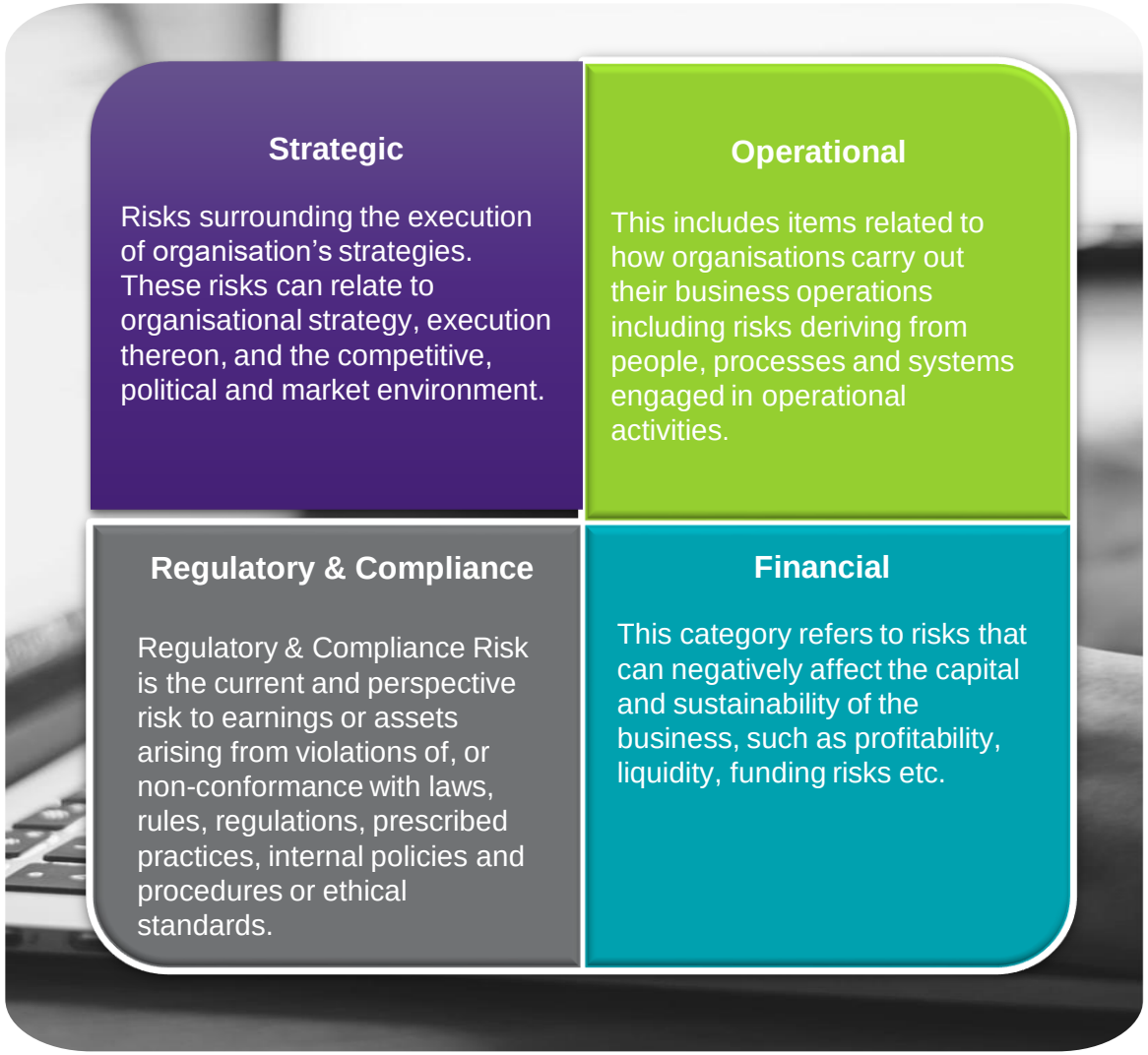
An effective ERM framework comprises tools designed to identify, assess, monitor and report key risks as well as Frameworks and Policies which articulate relevant risk governance roles and processes.

Risk Appetite is a key component of the ERMF

Risk Assessment is a key component of the Risk Management process

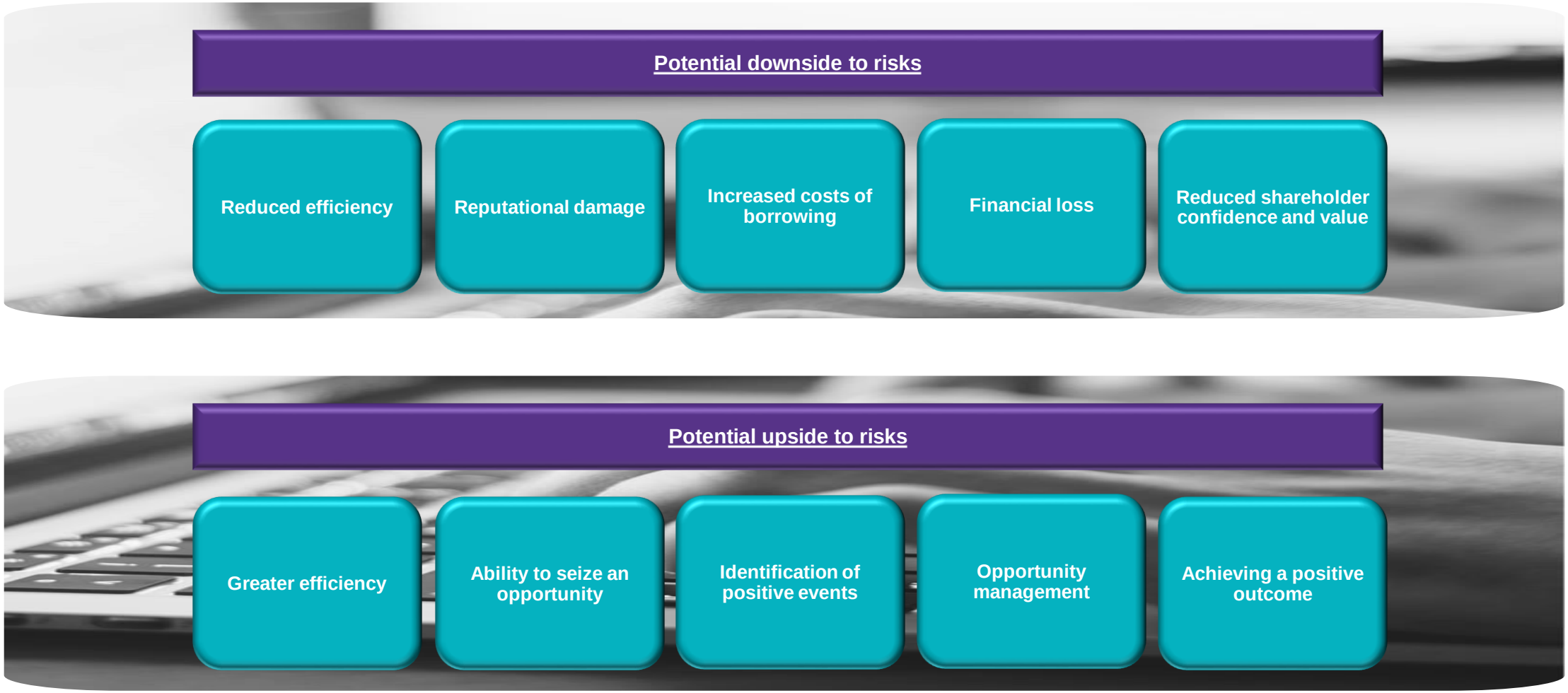
Enterprise Risk Management

Risk Categories

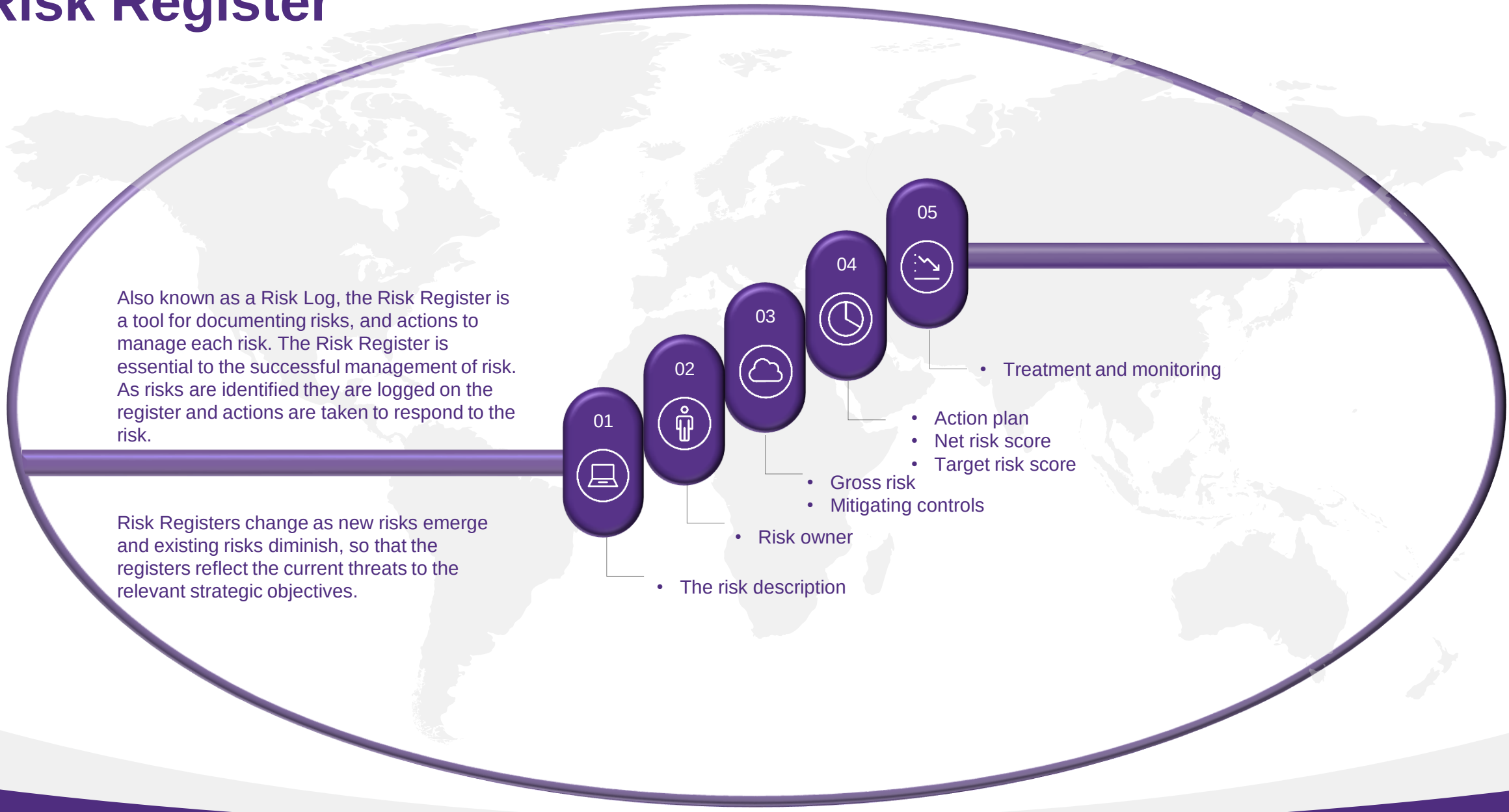


Enterprise Risk Management

Impact of Risk



Risk Register



Also known as a Risk Log, the Risk Register is a tool for documenting risks, and actions to manage each risk. The Risk Register is essential to the successful management of risk. As risks are identified they are logged on the register and actions are taken to respond to the risk.

Risk Registers change as new risks emerge and existing risks diminish, so that the registers reflect the current threats to the relevant strategic objectives.

01

- The risk description

02

- Risk owner

03

- Gross risk
- Mitigating controls

04

- Action plan
- Net risk score
- Target risk score

05

- Treatment and monitoring

Illustrative Risk Register

1. Risk details and Inherent Risk Rating

Risk Detail					Inherent Impact	Inherent Probability	Inherent Impact RAG	Inherent Impact Score
Risk ID	Risk Category	Process	Risk Description	Risk Owner				
CR 13	Operational Risk	Operational Resilience	The level of reliance on a small team of senior leadership and key subject matter experts heightens operational resilience risk materially for the Institute.	MD / Board	Moderate	Likely	High	12

2. Controls and Residual Risk Rating

Control ID	Actual key controls	Control Owner/ Operator	Control Frequency	Residual Impact	Residual Probability	Residual Impact RAG	Residual Probability Score
C 13.1	A SLT succession plan exists and is reviewed annually by the CEO and the Board	CEO/ Board	Annual	Minor	Possible	Low	4

3. Remedial Actions

Action Required	Action Owner	Action Due Date
HR Director to finalise the analysis and identification of resources that could potentially be placed into current SME roles.	HR Director	xx

Risk Reporting

Risk reporting is the vehicle for communicating the value that the Risk function brings to an organisation. It allows for pro active risk management as organisations identify and escalate issues either as they arise, or before they are realised to take a proactive approach to managing risks. Effective risk reporting should focus on how risk activities impact individual business unit and enterprise risk profiles.

ensures risk management is embedded into leadership, decision making, oversight and business operations

focuses on exceptions - and critically considers their underlying causes

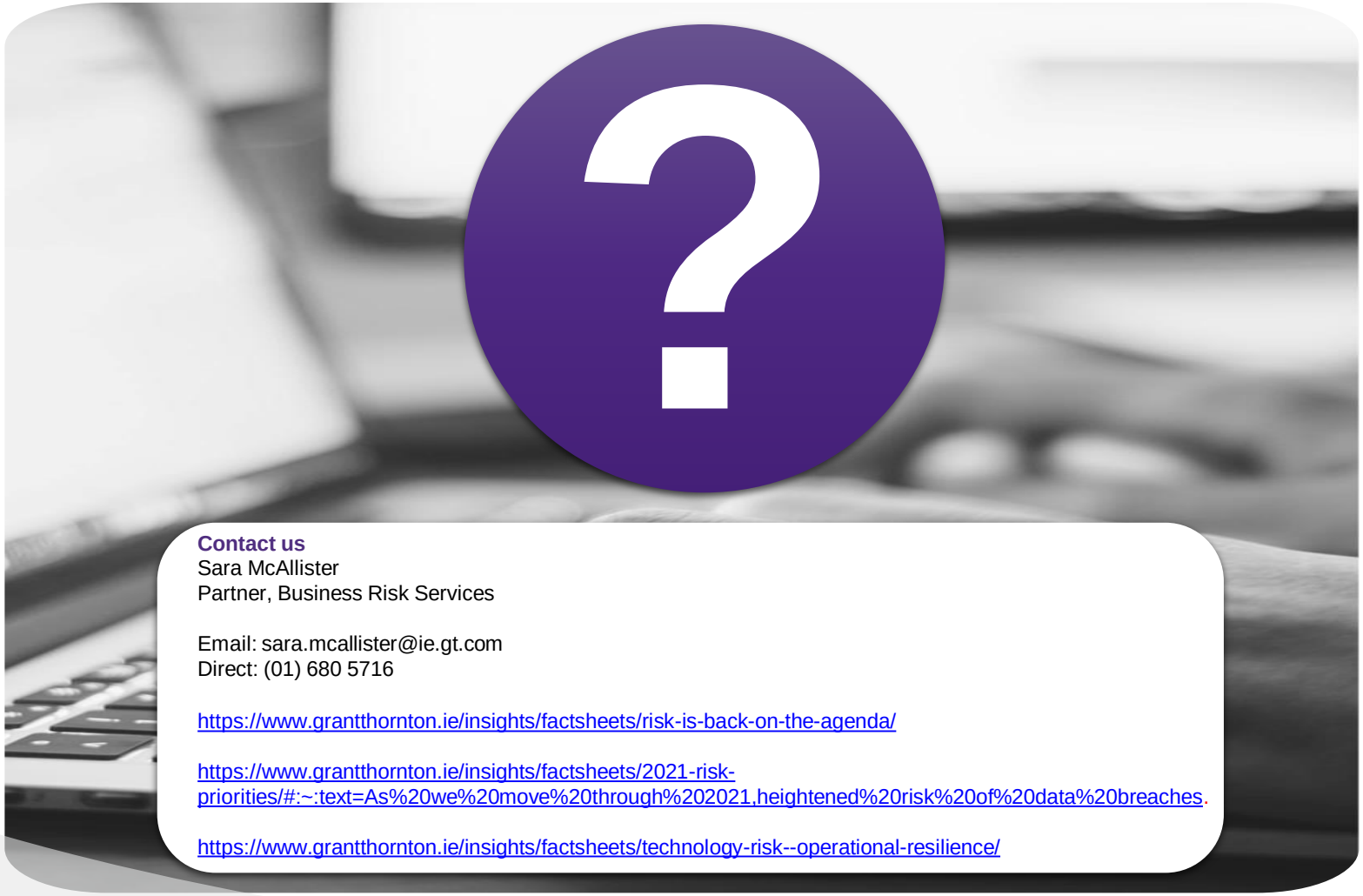
considers retrospective results as a means for learning and foresight of business risks before they occur

provides assurance to regulators, management and to Boards

provides transparency over exposures promoting continuous improvement – as areas of concern within the organisation are highlighted.

Using ERM to Balance Risk & Reward

Questions?



Contact us
Sara McAllister
Partner, Business Risk Services

Email: sara.mcallister@ie.gt.com
Direct: (01) 680 5716

https://www.grantthornton.ie/insights/factsheets/risk-is-back-on-the-agenda/

https://www.grantthornton.ie/insights/factsheets/2021-risk-priorities/#:~:text=As%20we%20move%20through%202021,heightened%20risk%20of%20data%20breaches.

https://www.grantthornton.ie/insights/factsheets/technology-risk--operational-resilience/