IIA Nordic Baltic cooperation project

GOOD PRACTICE GUIDELINES FOR THE ENTERPRISE RISK MANAGEMENT FUNCTION

2020

Why were the guidelines developed?

1. Set a generally accepted benchmark
   - strengthening the development of the risk management profession in the Nordic and Baltic countries and contribute to achieving the following IIA mission:
     “Research, disseminate, and promote knowledge concerning internal auditing and its appropriate role in control, **risk management**, and governance to practitioners and stakeholders”

Why were the guidelines developed?

2. Assist internal audit in discharging the following activities:
   - IA “must evaluate the effectiveness and contribute to the improvement of **risk management processes**” *IPPF 2120*
   - IA must assess and make appropriate recommendations to improve the organization’s governance processes for:
     - Making strategic and operational decisions.
     - **Overseeing risk management** and control
       IPPF 2110

Comparison IA and ERM

Enterprise Risk Management (ERM)

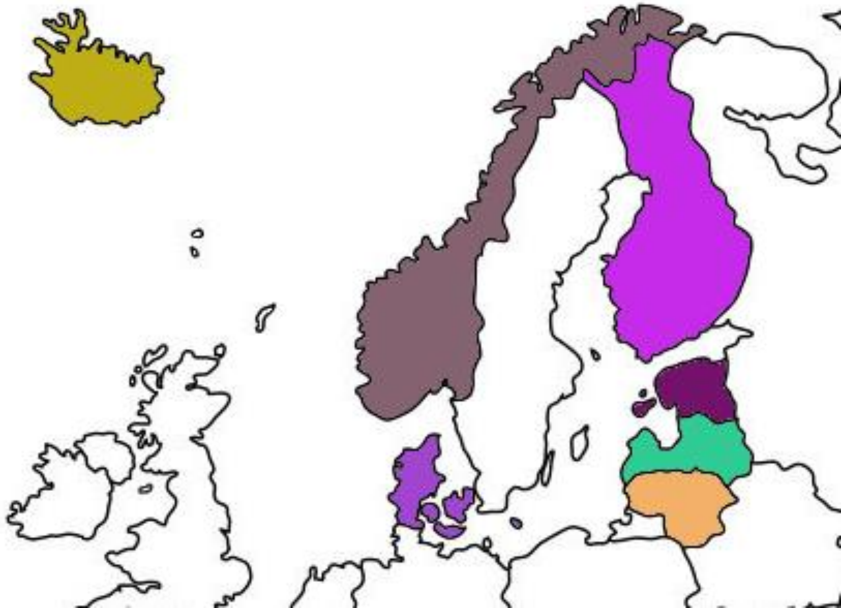
- Developing over last 15-20 years
- No internationally accepted standardsetting and professional association
- Standard for risk management ISO 31000 and COSO framework for ERM

Internal audit (IA)

- Institute of Internal Auditors established more than 80 years ago
- Global professional organisation and standardsetting body
- Board member of COSO author of internationally accepted frameworks for internal control and ERM

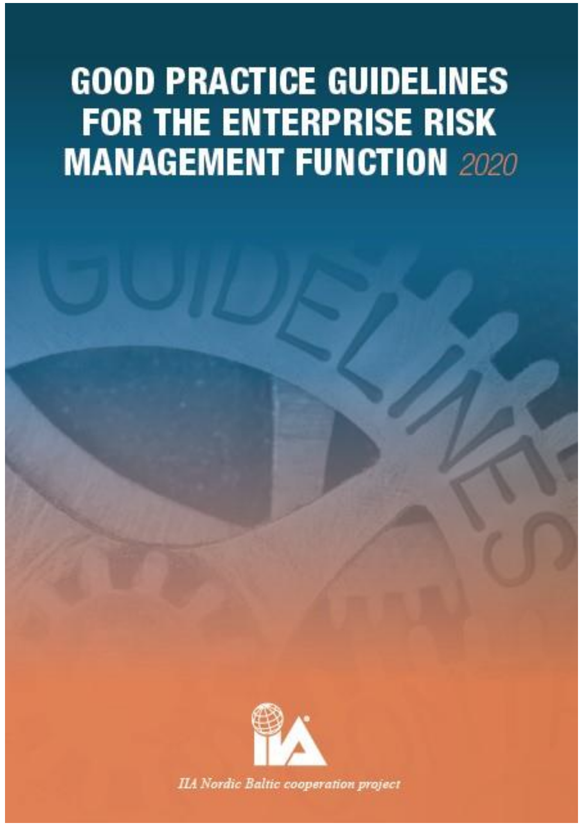
The guidelines

- Originally developed by IIA Norway but revised and expanded in a working group involving the participation of 7 Nordic and Baltic countries:



Progress through sharing!

Good practice guidelines for the ERM function



GOOD PRACTICE GUIDELINES FOR THE ENTERPRISE RISK MANAGEMENT FUNCTION 2020

IIA Nordic Baltic cooperation project

Process

- Developed further Guidelines for the Risk Management function from IIA Norway
- Working group with members from each country

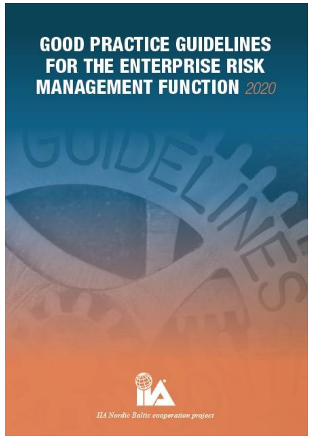
Intended audience

- Organisations that would like to either establish an Enterprise Risk Management function, or develop further their existing risk management function

Main changes made in the working group

- Explicitly state **Enterprise** Risk Management
- Role defined as a CRO role
- Cooperation between 2nd and 3rd Lines of Defence
- Re-structured to put guidance on specific risk management topics in appendices
- Additional guidance topics provided

Good practice guidelines for the ERM function



GOOD PRACTICE GUIDELINES FOR THE ENTERPRISE RISK MANAGEMENT FUNCTION 2020

IIA Nordic Baltic cooperation project

1 **Introduction**

1.1 The purpose of this guidance

1.2 The concept of risk

1.3 Enterprise Risk Management (ERM)

1.4 The RM responsibilities of governing bodies and organisational levels

1.5 The relationship between risk management, internal control and governance

2 **Important elements of the ERM function**

2.1 The ERM function's tasks and responsibility

2.2 The Board's responsibility and communication with the Board

2.3 Grounded in the Executive Management

2.4 Risk appetite

2.5 "Risk gaps"

2.6 Risk management, Executive Management and decision-making

3 **Organisation and segregation of duties**

3.1 The three lines of defence

3.2 Co-operation between 2nd and 3rd lines of defence

3.3 The position of the Enterprise Risk Management function in the organisation

3.4 Mandate, authority, competency and resources

3.5 Independence and integrity

3.6 Access to information

3.7 Remuneration and incentive system

3.8 Reporting requirements

3.9 Outsourcing the ERM function

Appendix 1 A practical approach to ERM and tools for developing risk management in an organisation

Appendix 2 Risk maturity

Appendix 3 Risk in decision making

Appendix 4 Risk appetite

Appendix 5 Questions a Board may ask

Appendix 6 ERM in the public sector

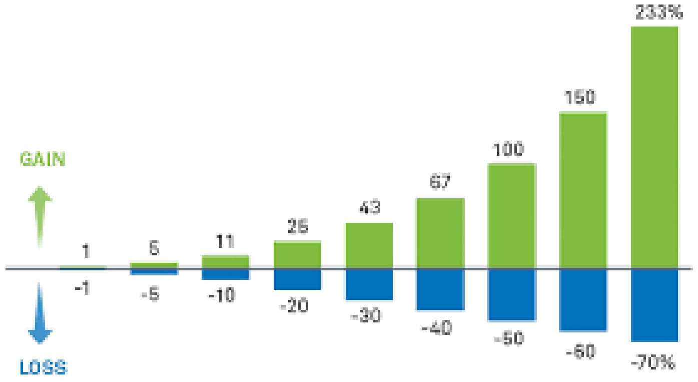
Appendix 7 Risk reporting

Guidelines for the ERM function

1. INTRODUCTION

1.2 Risk

- Some define risk only in terms of "unwanted events" i.e. downside



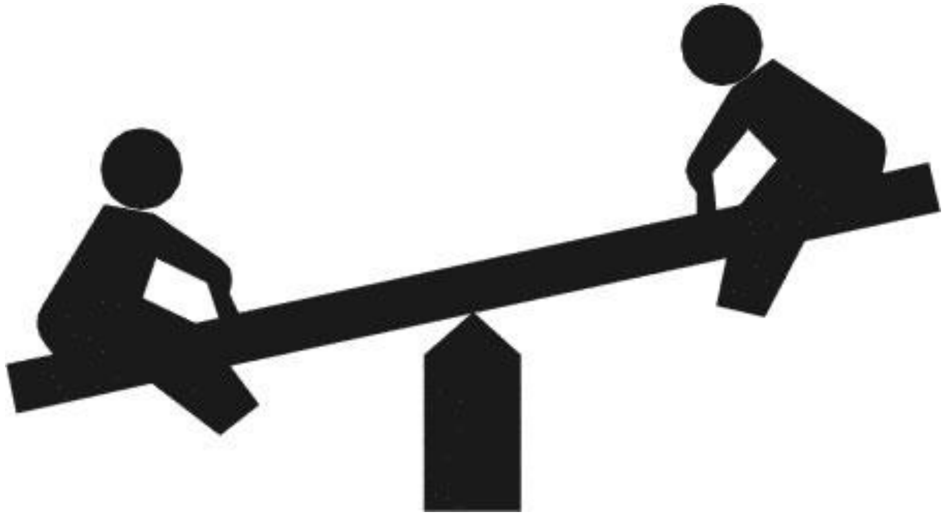
Source: BlackRock. For illustrative purposes only.

- Evaluating positive outcomes just as important in ERM.
- The objective of ERM is to maintain risk at an acceptable level and ensure the best possible balance between threats and opportunities.

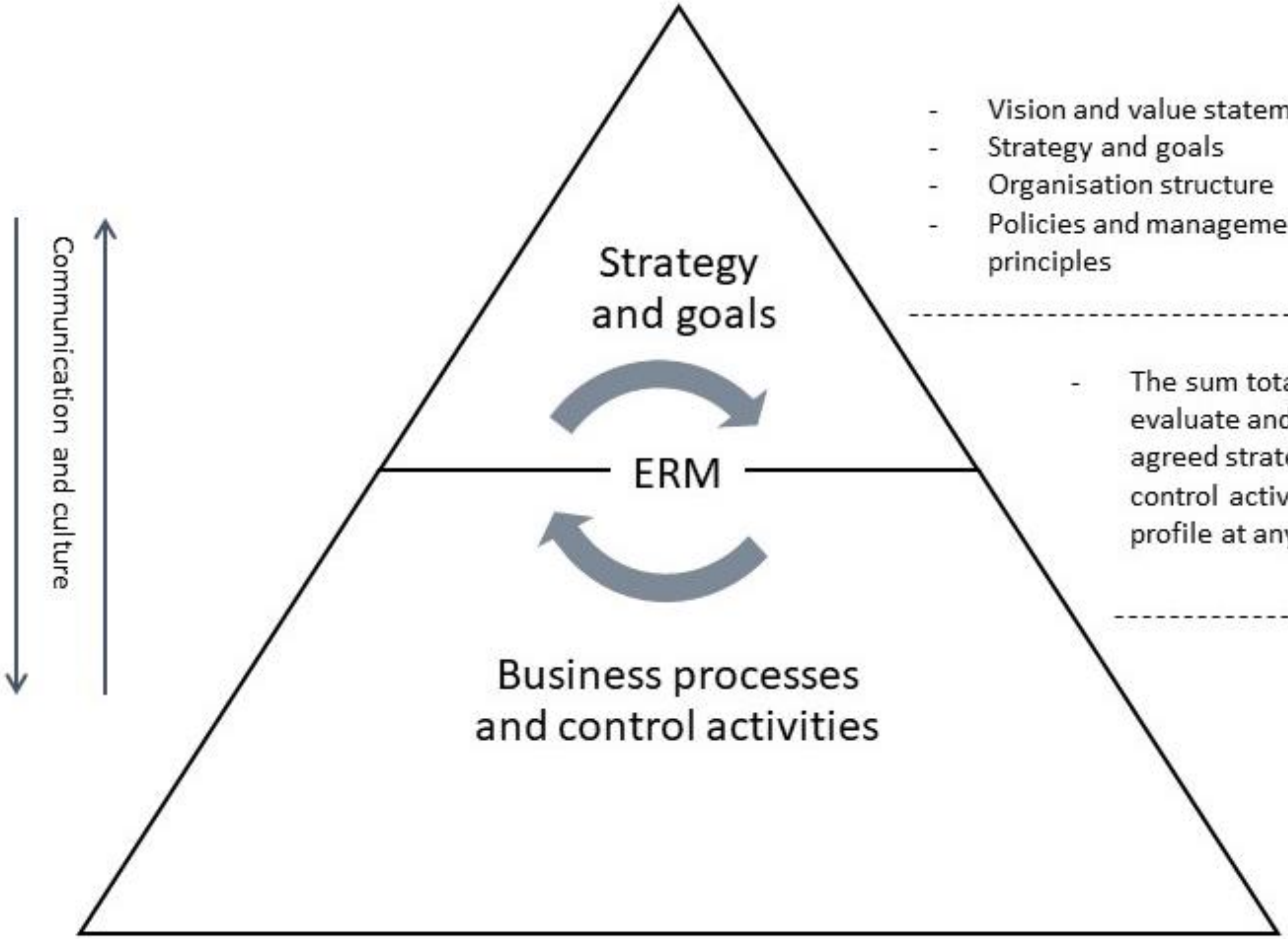
1.3 Enterprise Risk Management (ERM)

ERM ensures:

- Risk exposure balanced against achievement of the organisation’s objectives
- Appropriate management of assets
- The best possible basis for decision making



1.3 What is ERM?


Communication and culture
Strategy and goals
ERM
Business processes and control activities

- Vision and value statement
- Strategy and goals
- Organisation structure
- Policies and management principles

- The sum total of activities established to evaluate and ensure alignment between agreed strategies, business processes and control activities within the context of the risk profile at any given point in time

- Operational business processes
- Monitoring activities
- Control and oversight activities
- Reporting activities

1.4 Risk management takes place at various levels

Focus		Impact	Type of deviation	Type of risk management	
Focus	Enterprise	For the enterprise	Explicitly expressed at the enterprise level	Enterprise Risk Management (ERM) - includes holistic view of TRM and IRM	- The "owner" perspective - Priority at the portfolio level
			Not explicitly expressed at the enterprise level	Task Risk Management (TRM)	- Project manager focus: Deliverables in line with project goals (cost/time/quality)
	Individual	For an individual (Manager or employee)	Compensation and/or recognition	Individual Risk Management (IRM)	- Manager/employee is "ruled" by the requirement to achieve objectives in own scorecard

1.4 Risk management and internal control

Risk management and internal control are concepts that are frequently mentioned in conjunction.

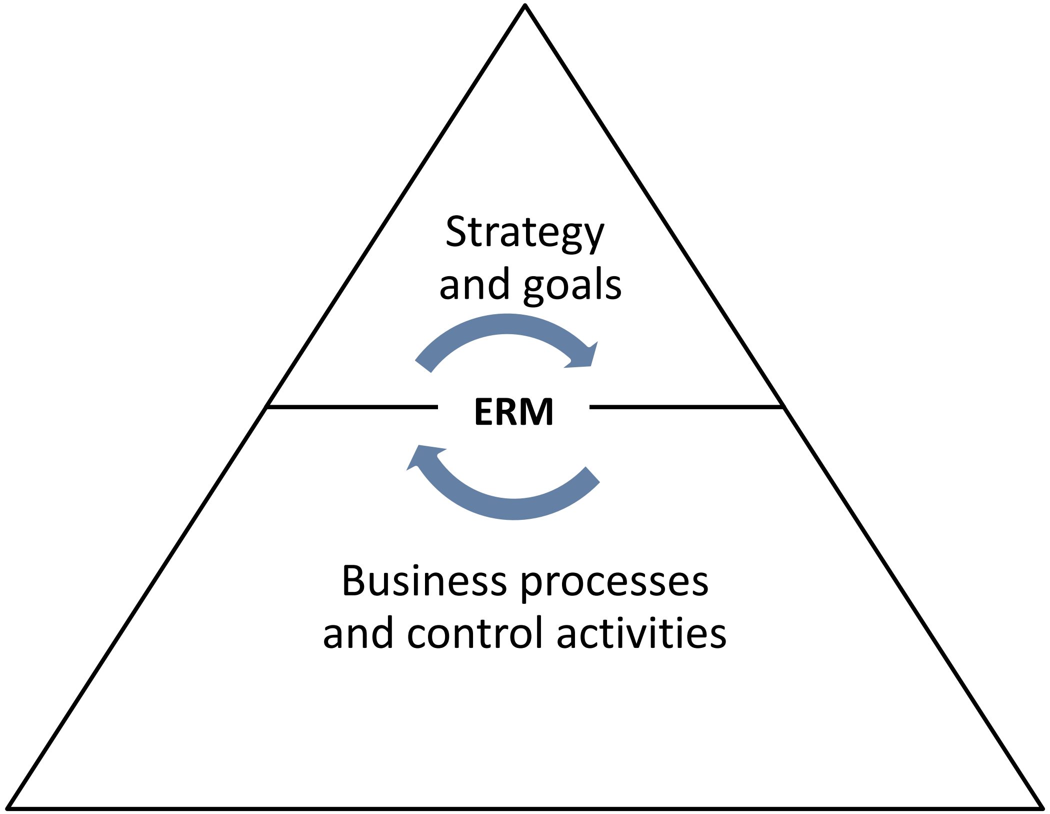
The concepts are often perceived too narrowly and separately to one another.

Risk management is more than the analysis and reporting of downside risk

Internal control concerns the management of an enterprise and is therefore not limited to specific control activities

Internal control may be looked upon as the consequence or a sub-process of ERM.

This sub-process can be defined as the sum total of management and control mechanisms.



IIA Nordic Baltic cooperation project

Guidelines for the ERM function

2. THE RISK MANAGEMENT FUNCTION – IMPORTANT PRINCIPLES

2.1 The function’s tasks and responsibilities

The guidelines focus on the ***«ERM function»***

In an enterprise it will be the Board or the highest decision making body that will ensure that the enterprise has established adequate risk management and internal controls.

The Chief Executive has overall operational responsibility for risk management. In their daily tasks all managers shall ensure that there is adequate risk management and internal control within their areas of responsibility in line with the organisation’s overall objectives.

2.1 The Chief Risk Officer (CRO)

- *Assists the organisation in designing and implementing efficient and effective processes to identify, analyse and treat risk.*
- *A standalone responsibility*
  - *to monitor the risk profile*
  - *to flag developing trends for existing risks and potential consequence of new threats/opportunities*

- Monitors and reviews the performance of risk management tasks taken as a whole
- Assists line management in communicating relevant risk information

Guidelines
Framework and principles
Strategy
Competency
Terminology
Tools
Ongoing communication
Reporting

2.1 CRO

Relevant responsibilities:

- Provides risk management techniques and assessments in relation to *strategy*-and *objective-setting* tasks.
- Establishes operational *guidelines* for risk management
- Prepares a *framework* for risk management
- Promotes the creation and preservation of risk management *knowledge*
- Establishes a common risk management *terminology*
- Develops a *methodology* for the identification, scoring, evaluation and monitoring of risk
- Assists management in the development of *risk reporting*
  - Setting of early warning flags through key risk indicators (KRI) or a trigger system for limit breaches
- Ensures ongoing *communication* to CEO and Board.

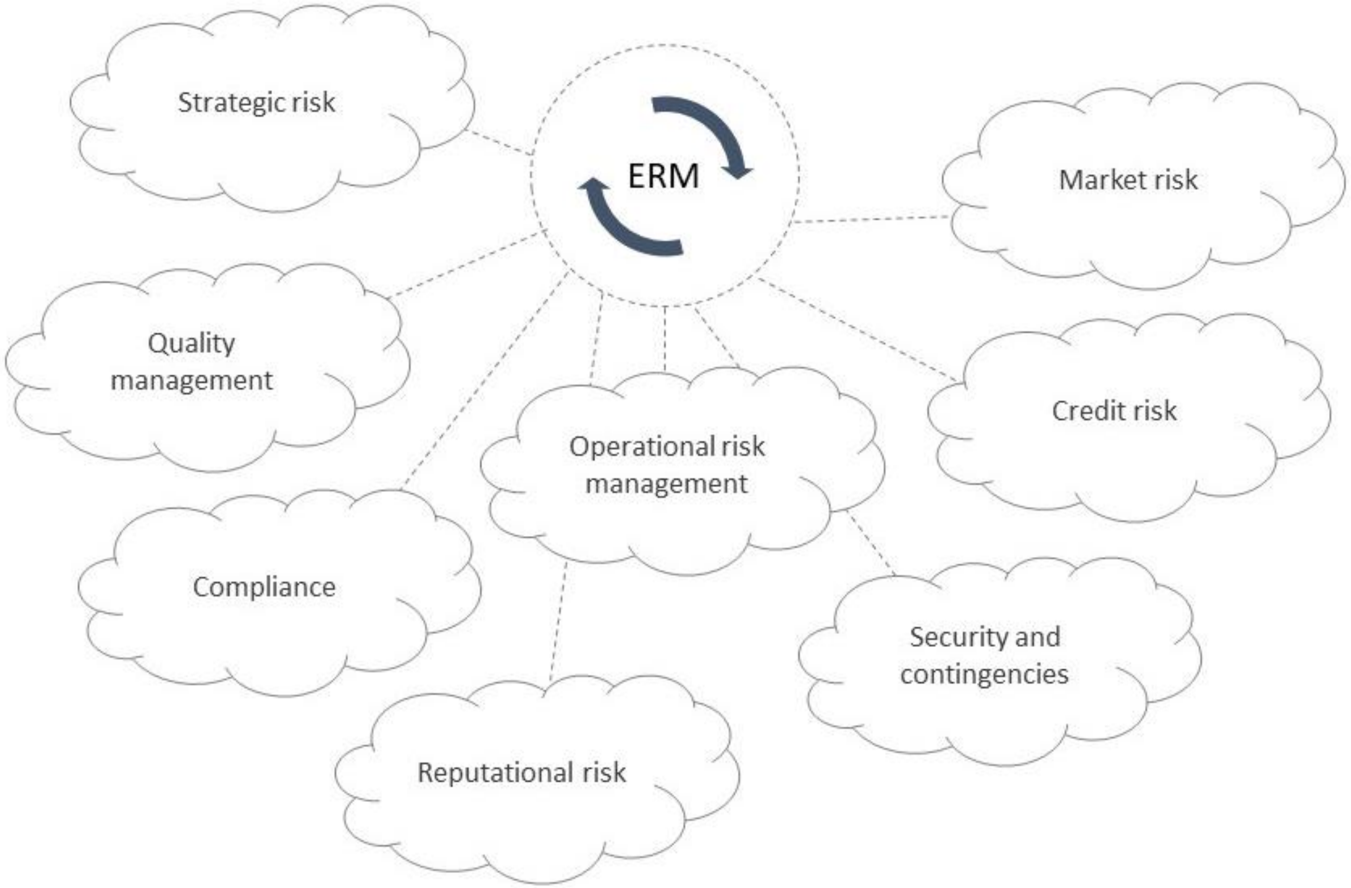
2.1 CRO

The CRO lays the groundwork for and monitors the implementation of:

- Effective *risk management principles* for senior management and assists risk owners in defining planned risk exposure
- Communication of *risk related information* to the organisation, including making expert pronouncements
- Principle that a *risk owner* has responsibility for the profits and losses associated with the defined risk.

2.1 CRO

The CRO should coordinate the risk management activities within the various professional and risk areas



2.2 and 2.3 Responsibility

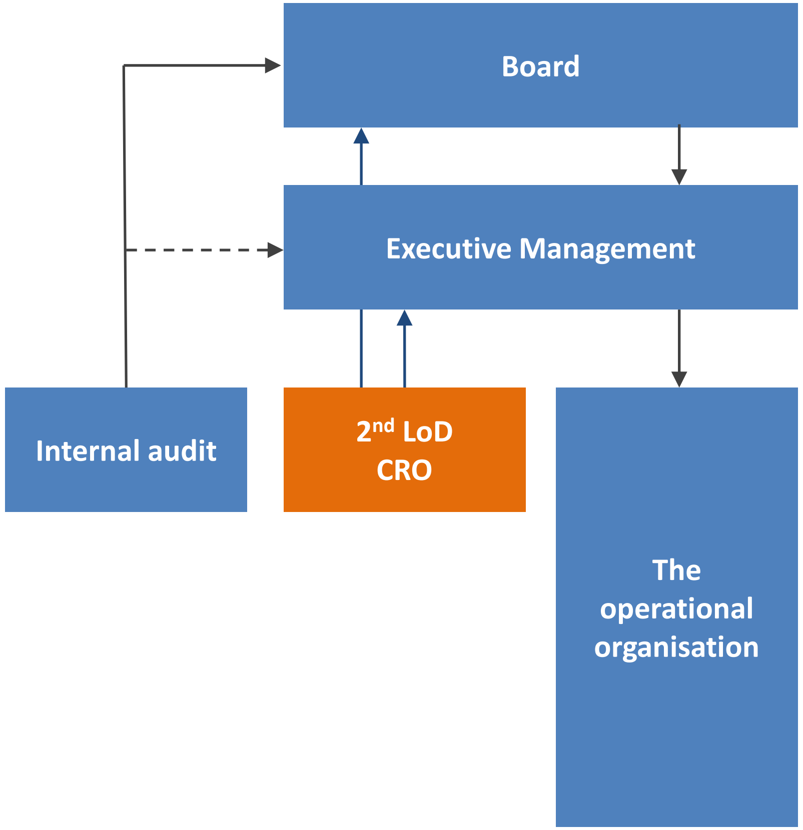
Board:

- Overall responsibility for legal compliance and sound risk management
- Sets risk appetite levels

Executive Management:

- Establishment and performance of sound risk management
- Sets job description and mandate for CRO
  - Position in the organisation
  - Mandate and resources = to the responsibilities, tasks and authority
  - Access to information
  - Reporting responsibility.

The CRO should have a direct reporting line to the Board



2.4 Risk appetite and 2.5 Risk gaps

The level of uncertainty an organisation is both willing and has the ability to take on, in order to carry out its activities and realise its goals

Risk appetite must be capable of being translated into operational practice.

There should be a common thread going through an organisation's various objectives, management limits, authorities and scope of action which accords with the total risk appetite and strategy.

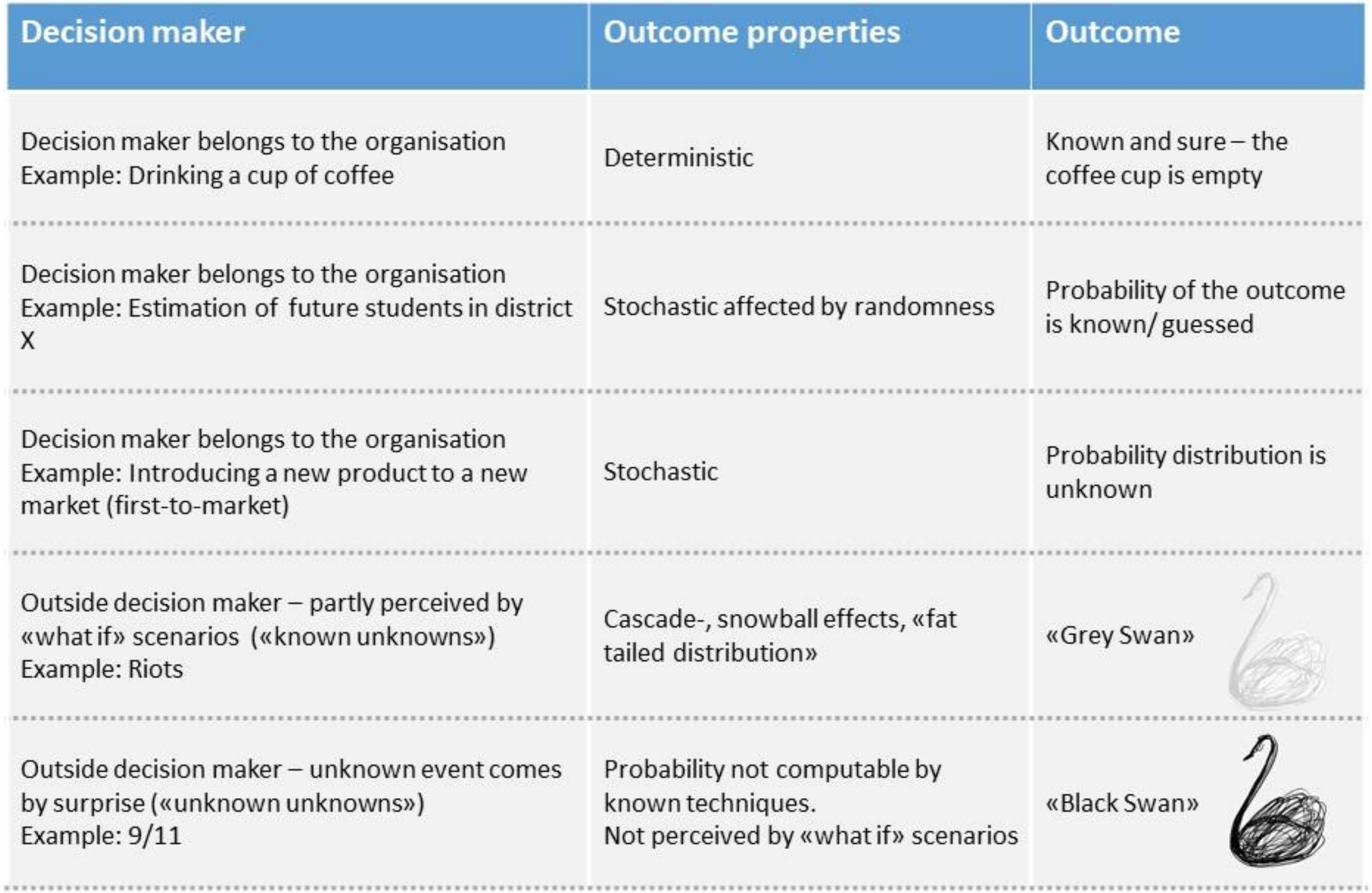
Risk appetite has both an aspect of desired situation and capability

«Risk gaps»

– the imbalance that can arise between actual risk exposure and expected return on investment

- the situation where inherent risk cannot be mitigated to below the risk appetite.

2.6 Risk management and uncertainty



Decision maker	Outcome properties	Outcome
Decision maker belongs to the organisation Example: Drinking a cup of coffee	Deterministic	Known and sure – the coffee cup is empty
Decision maker belongs to the organisation Example: Estimation of future students in district X	Stochastic affected by randomness	Probability of the outcome is known/ guessed
Decision maker belongs to the organisation Example: Introducing a new product to a new market (first-to-market)	Stochastic	Probability distribution is unknown
Outside decision maker – partly perceived by «what if» scenarios («known unknowns») Example: Riots	Cascade-, snowball effects, «fat tailed distribution»	«Grey Swan»
Outside decision maker – unknown event comes by surprise («unknown unknowns») Example: 9/11	Probability not computable by known techniques. Not perceived by «what if» scenarios	«Black Swan»

This illustration was originally published in "Y. Ayse B. Nordal, Risk Management Practices, Decision Making and Corporate Governance, Book of Proceedings", International May Conference on Strategic Management, University of Belgrade, May 2015.

2.6 Risk management and decision making

There is uncertainty attached to the outcome of a decision.

Sound risk management is about facilitating the best possible basis for making decisions.

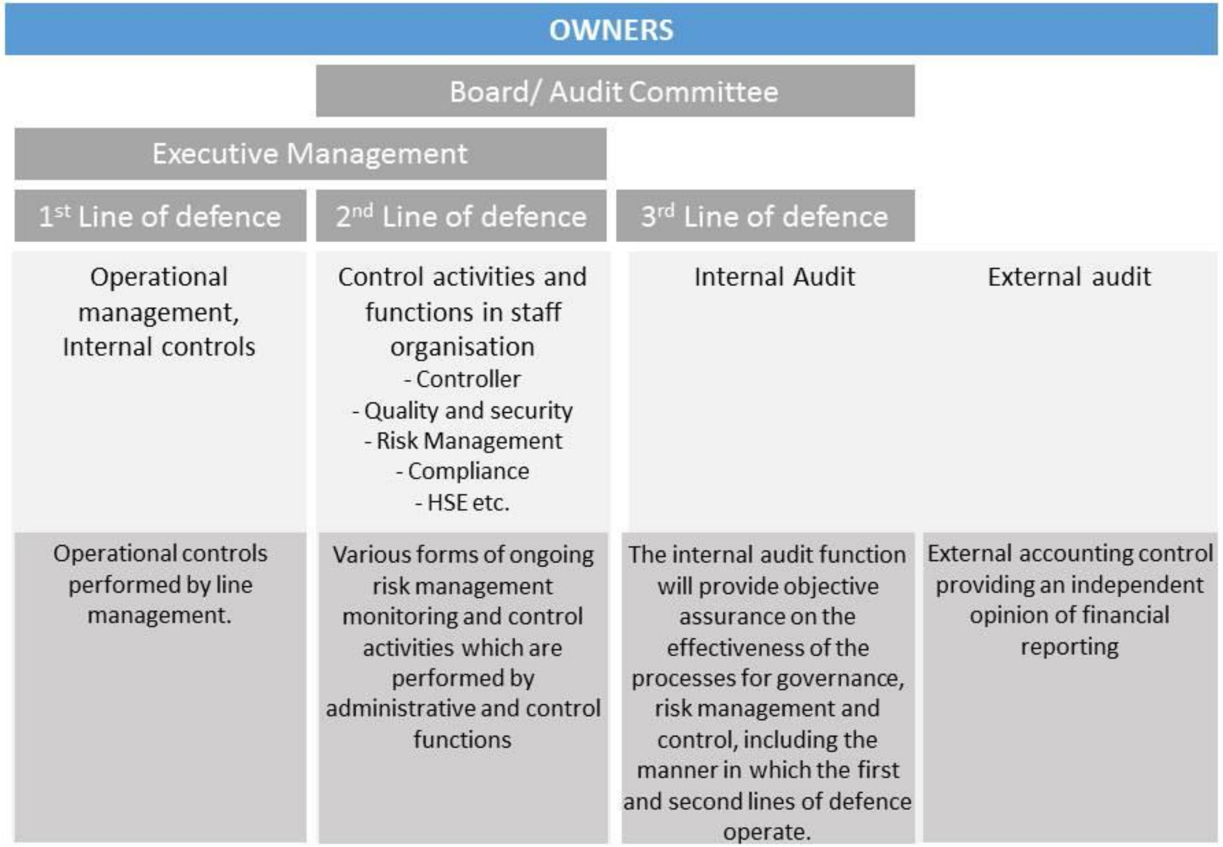
A better basis for decision making should also strengthen the ability to tackle a consequence that was not originally desired.

In connection with strategic risk it may be helpful to imagine 2 or 3 possible scenarios dependent on possible future developments in framework and market conditions and technological innovation.

Guidelines for the ERM function

3. ORGANISATION AND SEGREGATION OF DUTIES – IMPORTANT PRINCIPLES

3.1 The three lines of defence



OWNERS

Board/ Audit Committee

Executive Management

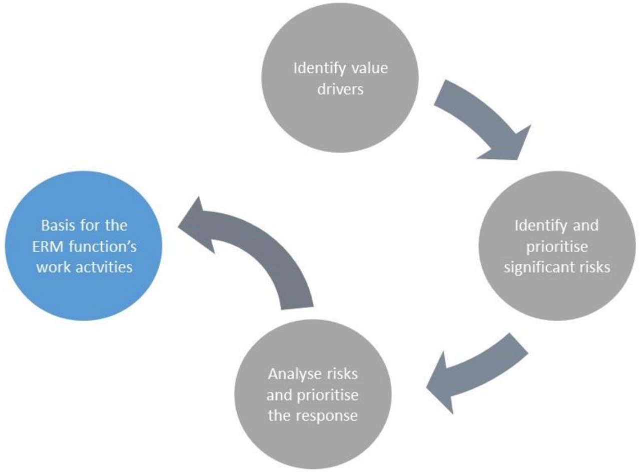
1st Line of defence	2nd Line of defence	3rd Line of defence	
Operational management, Internal controls	Control activities and functions in staff organisation - Controller - Quality and security - Risk Management - Compliance - HSE etc.	Internal Audit	External audit
Operational controls performed by line management.	Various forms of ongoing risk management monitoring and control activities which are performed by administrative and control functions	The internal audit function will provide objective assurance on the effectiveness of the processes for governance, risk management and control, including the manner in which the first and second lines of defence operate.	External accounting control providing an independent opinion of financial reporting

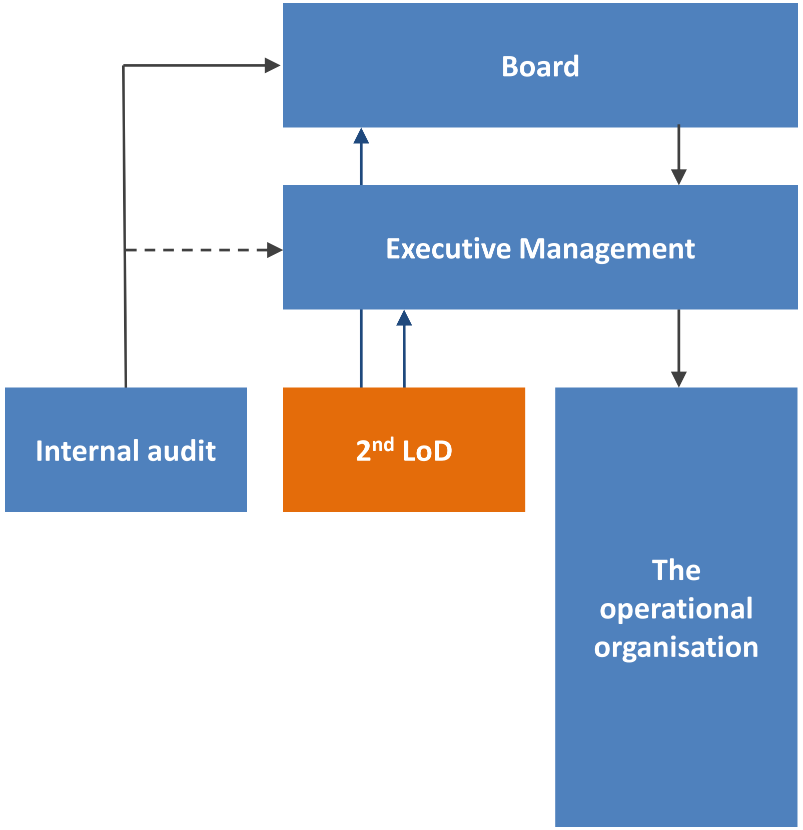
3.1 2nd LoD

A role which is both ***proactive*** *and* ***reactive****.*

Contributes to the development and performance of governance

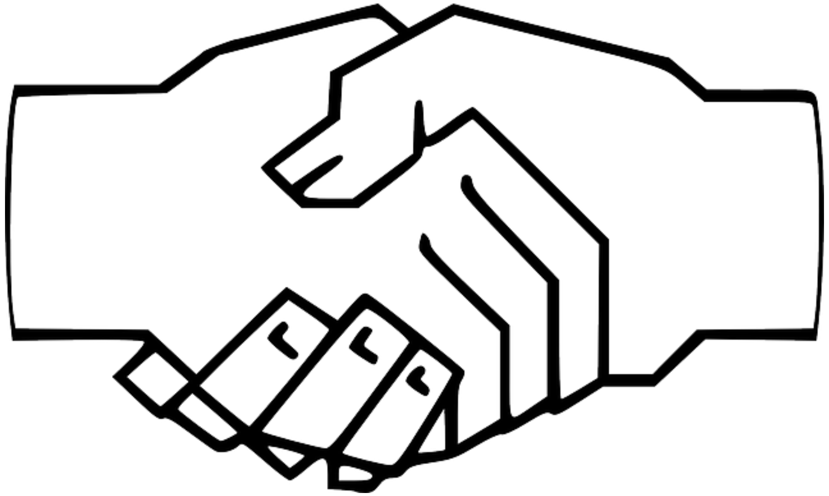
Identifies matters deviating from the desired development


Identify value drivers
Identify and prioritise significant risks
Analyse risks and prioritise the response
Basis for the ERM function's work actvities



3.2 Cooperation between 2nd and 3rd LoD

- Similarity:
  - Not responsible for the day to day operations
  - Common objective the organisation should develop successfully and sustainably.
- Documentation provided by the Risk Management and Compliance functions is important input to Internal Audit's risk-based plan
- Openness and trust can lead to:
  - IA better focus on those areas where monitoring by the Risk Management and Compliance functions are weaker
  - Quality assurance and feedback to 2nd LoD.



3.3 Organisational position and mandate

The Enterprise Risk Management function’s organizational positioning will vary dependent on the characteristics of the organisation and its maturity level in respect of ERM.

- *Organised into its own separate unit reporting to the Chief Executive on a par with other administrative functions*
- *Positioned together with other risk and control functions*
- *Included in another role description*

Irrespective of organisation the function requires adequate ***mandate, authority, competency and resources***

3.4 Authority, competency and resources

Senior position in the organisation

N.B. risk management is a profession which requires professional competency as well as a relevant background and experience

A professional career path will have a positive effect on the development of both the individual and the function

3.5 Independence and integrity
3.7 Remuneration and incentive system

People employed in and responsible for the organisation's Enterprise Risk Management function, should as far as possible be organised independently from operational activities.

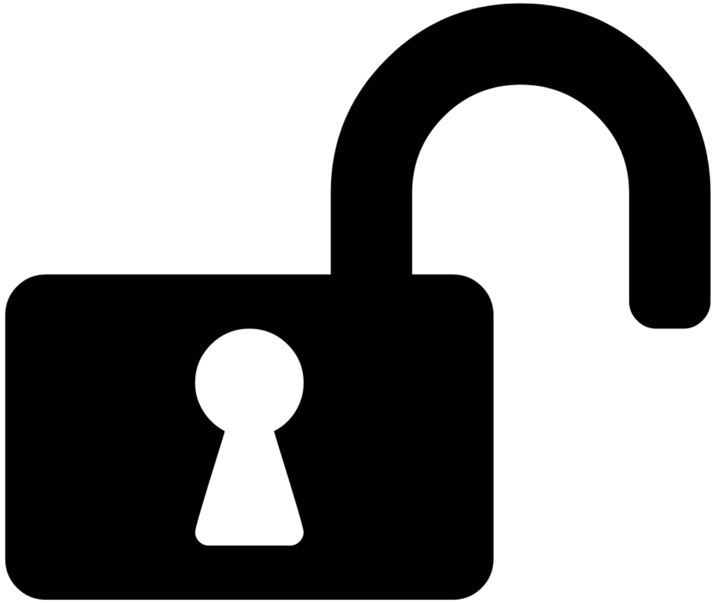
Employees working in the Enterprise Risk Management function must possess, in addition to a relevant professional competency, a high level of professional integrity.

The remuneration and incentive system for the Enterprise Risk Management function should not contain significant financial performance-based components that could lead to conflicts of interest and influence the objectivity of the staff working in the function.

3.6 Access to information

The Enterprise Risk Management function should have:

- access to required information regarding the organisation's operations and decisions.
- the right to participate in internal meetings as basis for:
  - performing reviews
  - monitoring activities



3.8 Reporting requirements

Need to provide:

- Regular reporting to Board and Executive Management

- Ad hoc reporting

3.9 Is outsourcing OK?

Management cannot outsource *responsibility* for risk management.

When outsourcing all or part of the function executive management must ensure that all the basic requirements are met.

Specific legislation may limit the possibility of outsourcing.

Most usual at the commencement of the process to establish ERM, helping build:

- Common language
- Common risk culture
- Well-functioning framework for ERM.

Summarising the key points

IIA Nordic Baltic cooperation project

Statement	Reference
1. Risk management is a line management responsibility	3.1 and 3.2
The ERM function:	
2. Ensures integration of risk management into decision-making	2.6
3. Maintains clear and open communication	2.6
4. Has a clearly defined mandate	3.4
5. Is organised independently and demonstrates professional integrity	3.3 and 3.5
6. Is granted access to all relevant information	3.6
7. Has no significant financial performance-based components to salary	3.7
8. Offers remuneration sufficient to attract and retain staff of satisfactory calibre	3.7

Appendices

Practical guidance in the following areas:

1. A practical approach to ERM and tools for developing RM in an organisation
2. Risk maturity
3. Risk in decision making
4. Risk appetite
5. Questions a Board may ask
6. ERM in the public sector
7. Risk reporting

N.B.:

Risk is there – why not manage it?

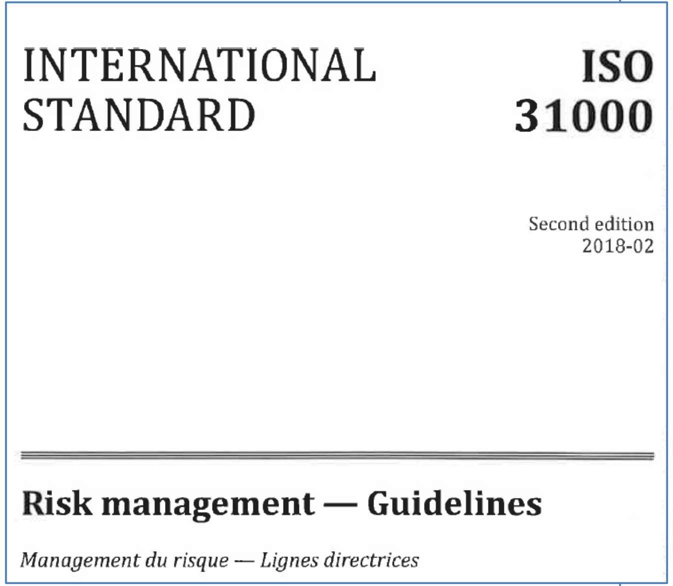
Guidelines for the ERM function

APPENDICES WITH PRACTICAL GUIDANCE

Appendix 1 - A practical approach to ERM
1. Framework and standards

Two standards / frameworks for ERM have received acceptance internationally:

1. *ISO 31000:2018 – Risk Management – Guidelines*
2. *COSO: 2017 Enterprise Risk Management – Integrating with Strategy and Performance*



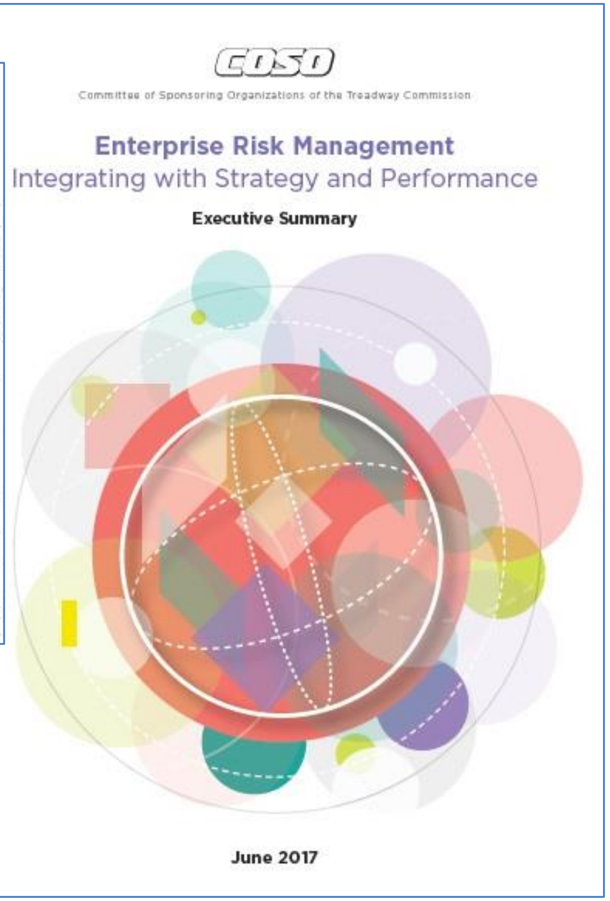
INTERNATIONAL STANDARD

ISO 31000

Second edition
2018-02

Risk management — Guidelines

Management du risque — Lignes directrices



COSO

Committee of Sponsoring Organizations of the Treadway Commission

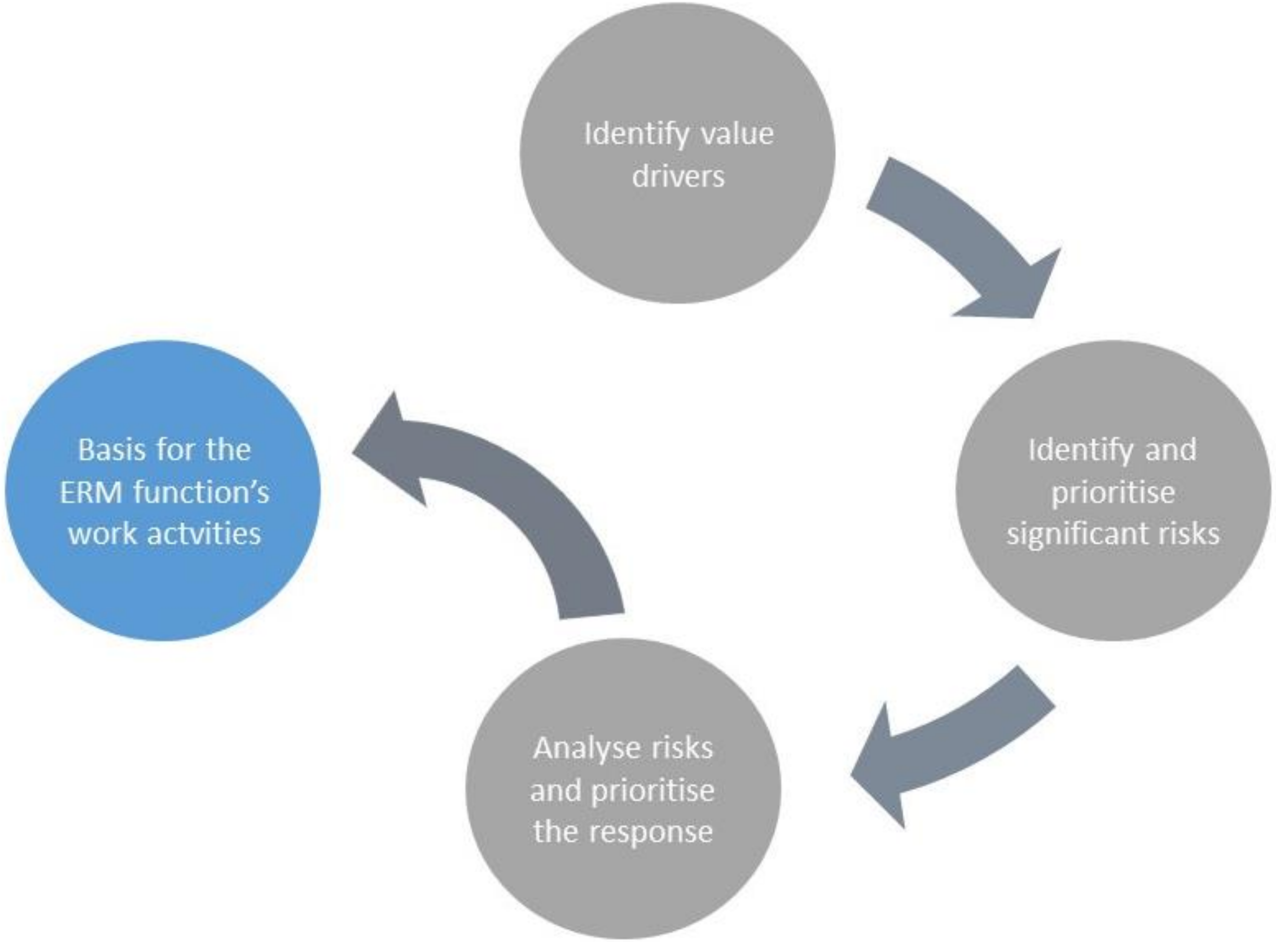
Enterprise Risk Management

Integrating with Strategy and Performance

Executive Summary

June 2017

Appendix 1 - A practical approach to ERM
3. Performing a high level assessment



Identify value drivers
Identify and prioritise significant risks
Analyse risks and prioritise the response
Basis for the ERM function's work actvities

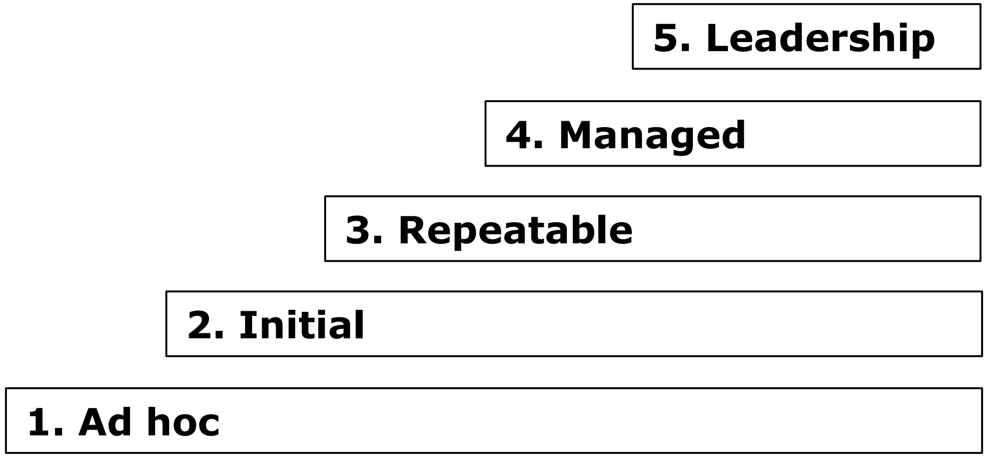
Appendix 1 - A practical approach to ERM

4. 17-point plan for the establishment of an ERM function in the organisation

5. Reasons for failure in the establishment of ERM

Appendix 2 - ERM maturity

- Traditional



5. Leadership

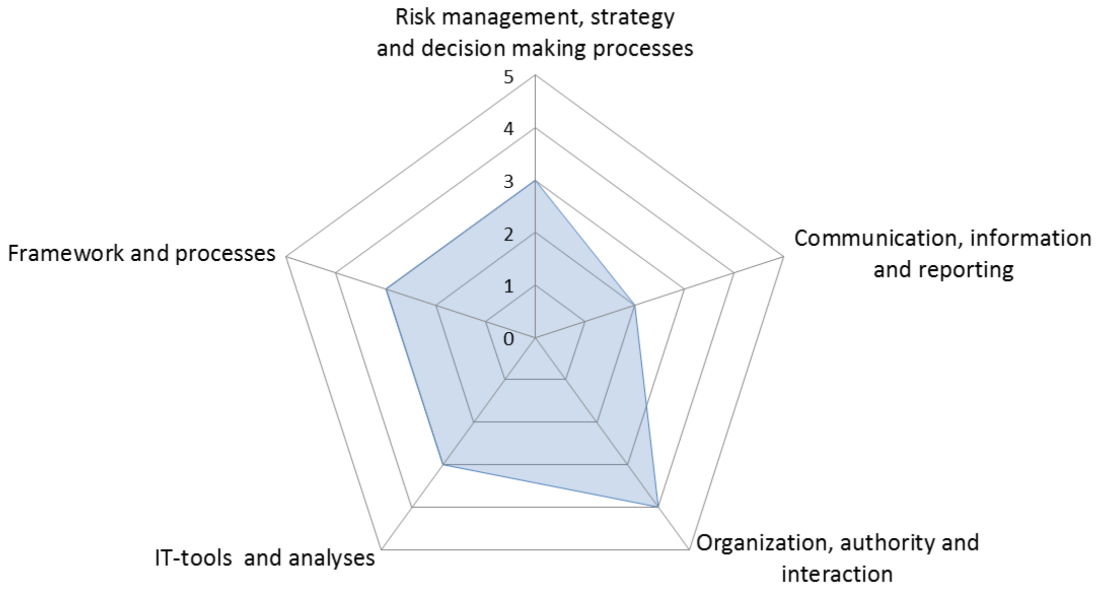
4. Managed

3. Repeatable

2. Initial

1. Ad hoc

- Fresh approach



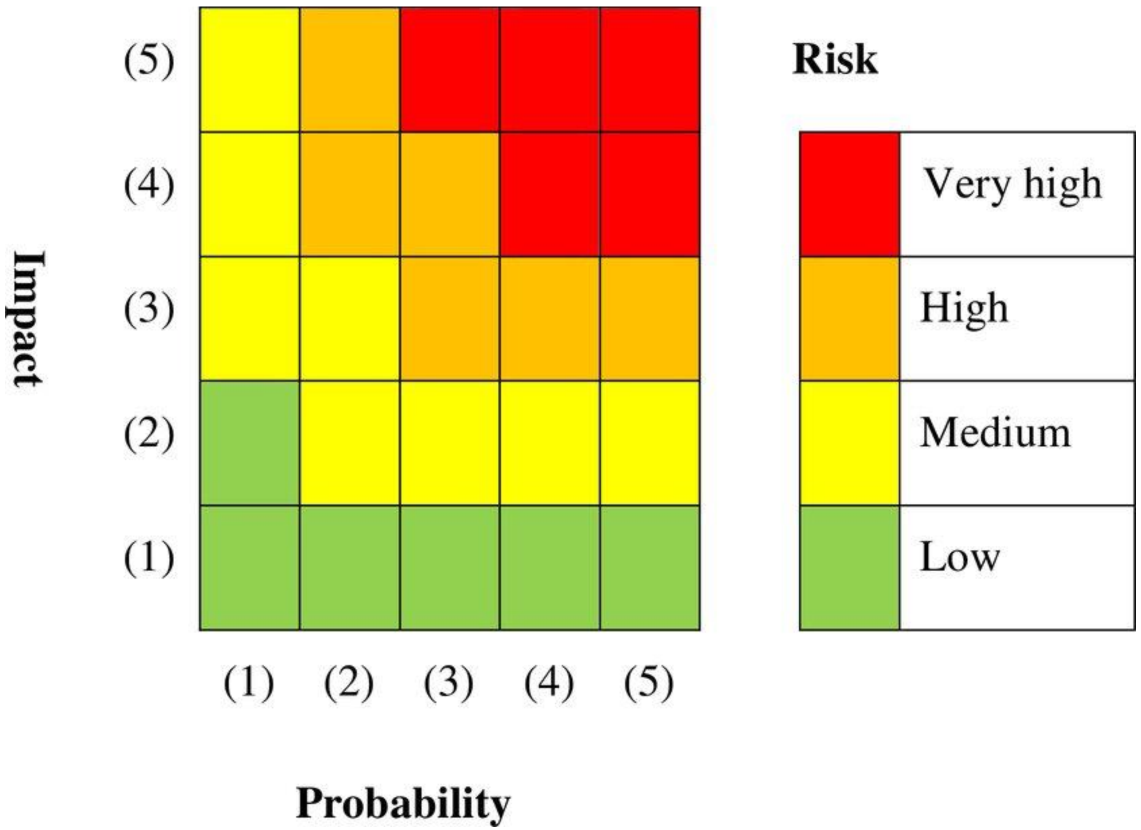
Appendix 3 – Risk and decision-making

1. Quantifying risks
2. Decisions and risk management involvement
    1. Day to day decisions
    2. Strategic decisions
    3. Contingency awareness

Appendix 4 – Risk appetite

1. Risk appetite v. Risk tolerance

2. Setting the risk profile



Impact					
(5)	🟨	🟧	🟥	🟥	🟥
(4)	🟨	🟧	🟧	🟥	🟥
(3)	🟨	🟨	🟧	🟧	🟧
(2)	🟩	🟨	🟨	🟨	🟨
(1)	🟩	🟩	🟩	🟩	🟩
	(1)	(2)	(3)	(4)	(5)
	Probability				

Risk

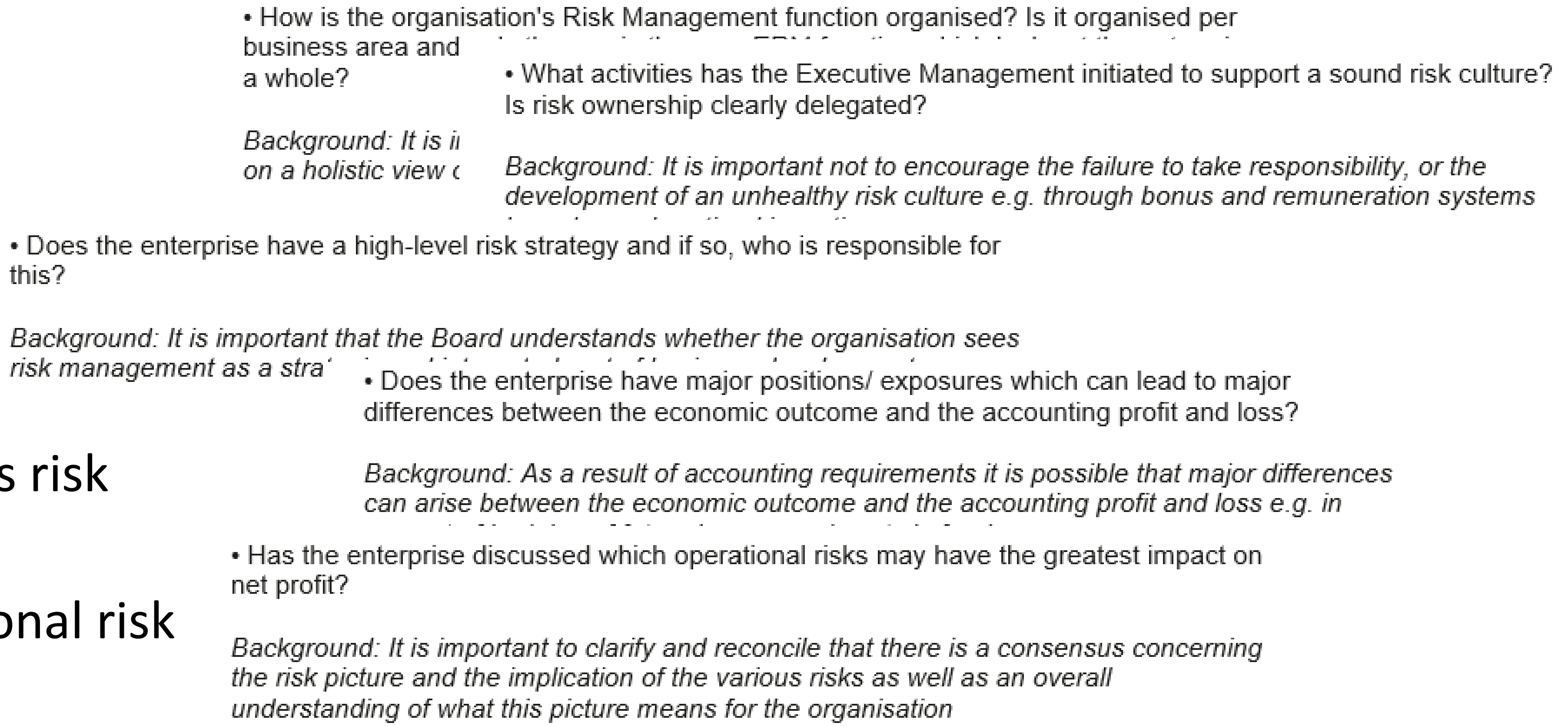
🟥	Very high
🟧	High
🟨	Medium
🟩	Low

Appendix 5 - Questions a Board may ask

to understand how an organisation controls its risks

IIA Nordic Baltic cooperation project

- Governance
- Risk management
- Compliance
- Managing business risk
- Managing operational risk



• How is the organisation's Risk Management function organised? Is it organised per business area and

a whole?

Background: It is i

on a holistic view

• What activities has the Executive Management initiated to support a sound risk culture? Is risk ownership clearly delegated?

Background: It is important not to encourage the failure to take responsibility, or the development of an unhealthy risk culture e.g. through bonus and remuneration systems

• Does the enterprise have a high-level risk strategy and if so, who is responsible for this?

Background: It is important that the Board understands whether the organisation sees risk management as a stra

• Does the enterprise have major positions/ exposures which can lead to major differences between the economic outcome and the accounting profit and loss?

Background: As a result of accounting requirements it is possible that major differences can arise between the economic outcome and the accounting profit and loss e.g. in

• Has the enterprise discussed which operational risks may have the greatest impact on net profit?

Background: It is important to clarify and reconcile that there is a consensus concerning the risk picture and the implication of the various risks as well as an overall understanding of what this picture means for the organisation

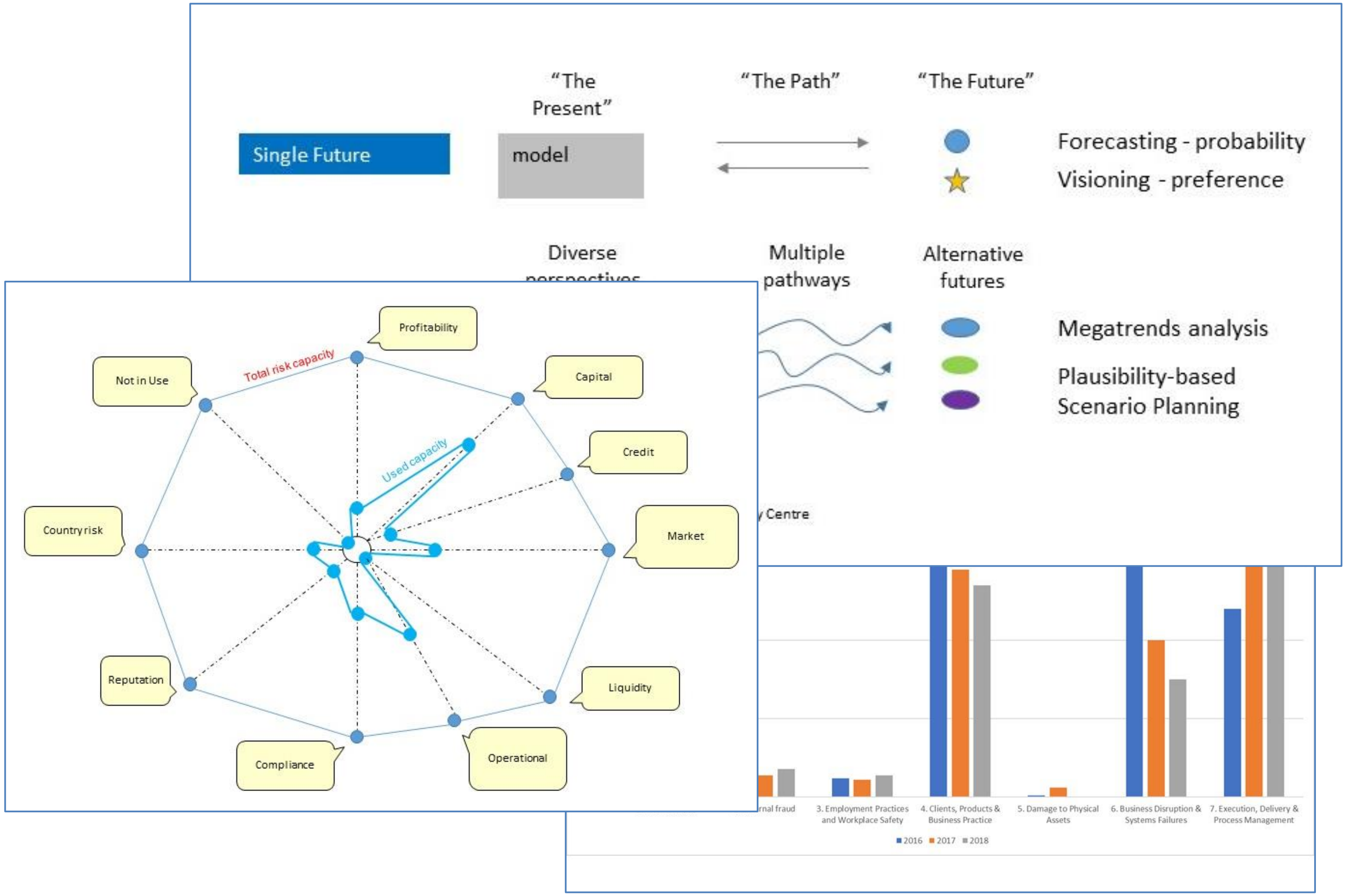
Appendix 6 - ERM in the public sector

1. Background
2. Risk definition
3. Managing risk reduction activities and effects in the public sector
4. Risk management and internal control
5. Risk culture
6. Risk appetite

Appendix 7 – Risk reporting

Reporting by risk categories:

1. Strategic
2. Business
3. Financial
4. Operational



"The Present"
"The Path"
"The Future"
Single Future
model
Forecasting - probability
Visioning - preference
Diverse perspectives
Multiple pathways
Alternative futures
Megatrends analysis
Plausibility-based Scenario Planning
Centre
Profitability
Capital
Credit
Market
Liquidity
Operational
Compliance
Reputation
Country risk
Not in Use
Total risk capacity
Used capacity
rnal fraud
3. Employment Practices and Workplace Safety
4. Clients, Products & Business Practice
5. Damage to Physical Assets
6. Business Disruption & Systems Failures
7. Execution, Delivery & Process Management
2016
2017
2018