Theoretical Background in Risk Management

April 2019

CV

Head of Audit and Risk Management (CRO)

Austrian Datacenter, 1500 employees, 7 affiliates,

Training and Consulting in Managementsystems

Preparation for Certifications (eg. IPMA, ONR 49000, ISO 31000)
Teaching at FH-Vienna, DU-Krems und HSO Executive in
St. Gallen, Bern and Zurich

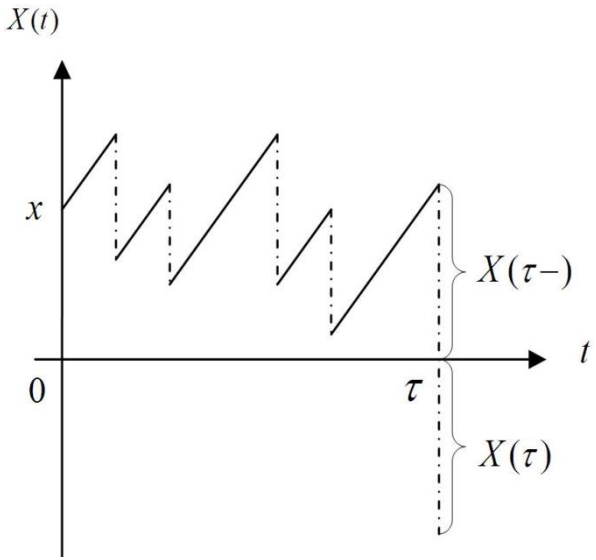
Continuing education

10/2017:	Certification to ITIL®
11/2014:	Re-certified Projectmanager to IPMA – B
11/2012:	CRMA Certification in Risk Management Assurance
04/2010:	MBA Project- and Processmanagement
11/2009:	Re-certified Projectmanager to IPMA – B
12/2007:	certified Riskmanager to ONR 49 000
10/2007:	Certified Projectmanager to PRINCE 2
1999-02:	PhD: Correlation of risks, Vienna
3-11/98:	ULG International Projectmanagement
1983-91:	Operating Informatics at TU, Vienna
1977-82:	HTL for Civil Engineering, Vienna

Overview

- Origins of Risk Management
- Inside Admiral Tirpitz
- History of Standardization in Risks
- What is a Risk?
- Some helpful Standards?
  - M.o.R. Management of Risk (UK Gvt)
  - RAMP Risk Analysis and Management for Projects (CE)
  - PRINCE2 PRojects IN Controlled Environments (UK)
  - PMI Project Management Institute (US)
  - IPMA Int. Project Mgmt Association ICB4 (EU, Pac Asia)
  - COBIT 5 Enterprise Risk Management
  - COSO Framework for Risk Management
  - ONR 49000 Austrian-Suisse Alternative
  - ISO 31000 Standard for Risk Management
- Checking any Risk Management System
- Risk Management for „Adults“

Risk Theory origins in the insurance industry



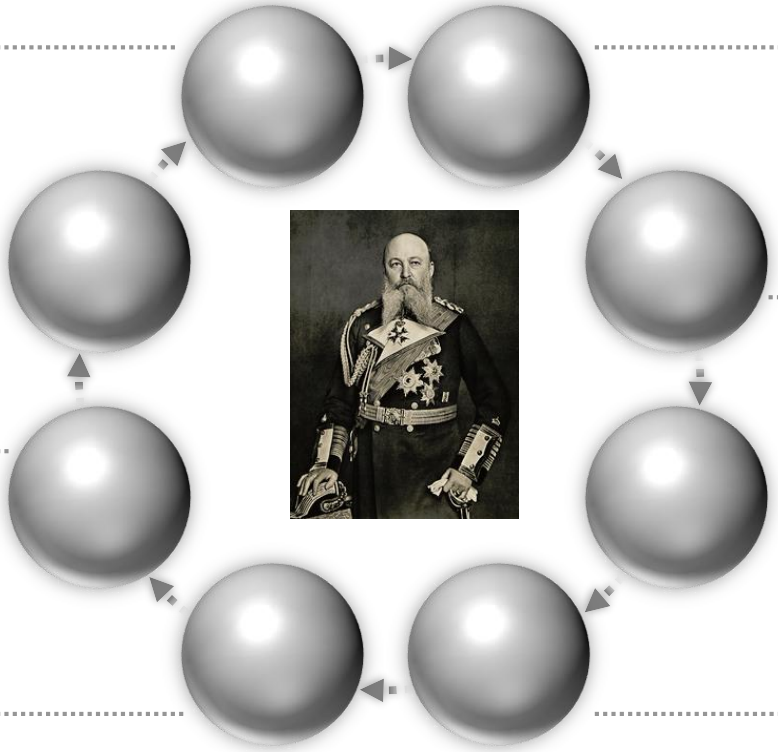
- In actuarial science and applied probability **ruin theory** uses mathematical models to describe an insurer's vulnerability to insolvency/ruin. In such models key quantities of interest are the probability of ruin, distribution of surplus immediately prior to ruin and deficit at time of ruin.
- The **Cramér–Lundberg model was introduced in 1903** by the Swedish actuary Filip Lundberg.
- The model describes an insurance company who experiences two opposing cash flows: incoming cash premiums and outgoing claims. Premiums arrive a constant rate $c > 0$ from customers and claims arrive according to a Poisson process with intensity λ and are independent and identically distributed non-negative random variables with distribution F and mean μ (they form a compound Poisson process).

…and in the military industry

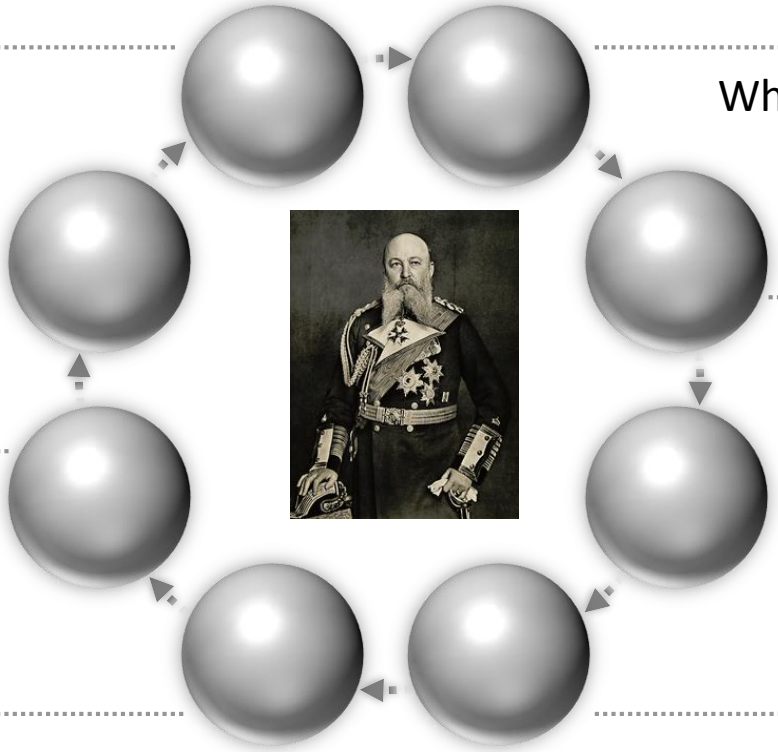
Admiral von Tirpitz, 1906

- *"A German fleet does not necessarily have to be strong enough to defeat the Royal Navy to push the UK towards a german-friendly naval - and overall Policy. It is already enough to build a fleet strong enough to make its destruction by Britain a "Pyrrhic Victory".*
- "*Britain cannot afford to engage in a belligerent confrontation with another Naval Power if, despite the numerical and qualitative inferiority of its fleet, it was strong enough to be destroyed by The Royal Navy, for its part, to destroy large parts of it*."
- From 1900 onward, when the so-called *Risikoflotte* ("risk fleet"—i.e., a deterrent for potential attackers) was established under the second navy law, it became obvious that the navy was intended not only for actual defense but also as an alliance asset in time of peace. The emperor and Tirpitz hoped to be able, through mounting financial and military pressure, to force Britain to loosen its alliances.

Inside Admiral Tirpitz…

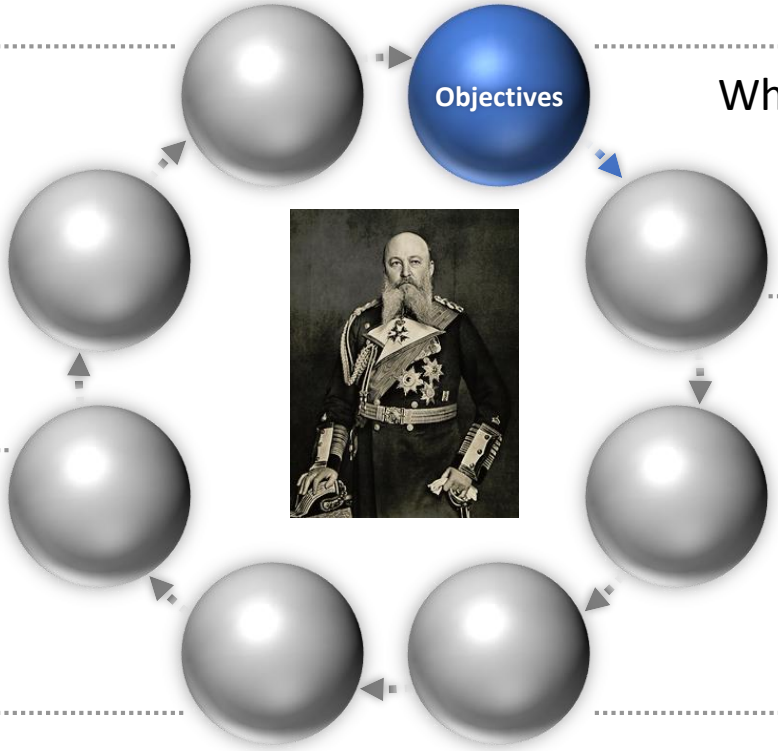


Inside Admiral Tirpitz…



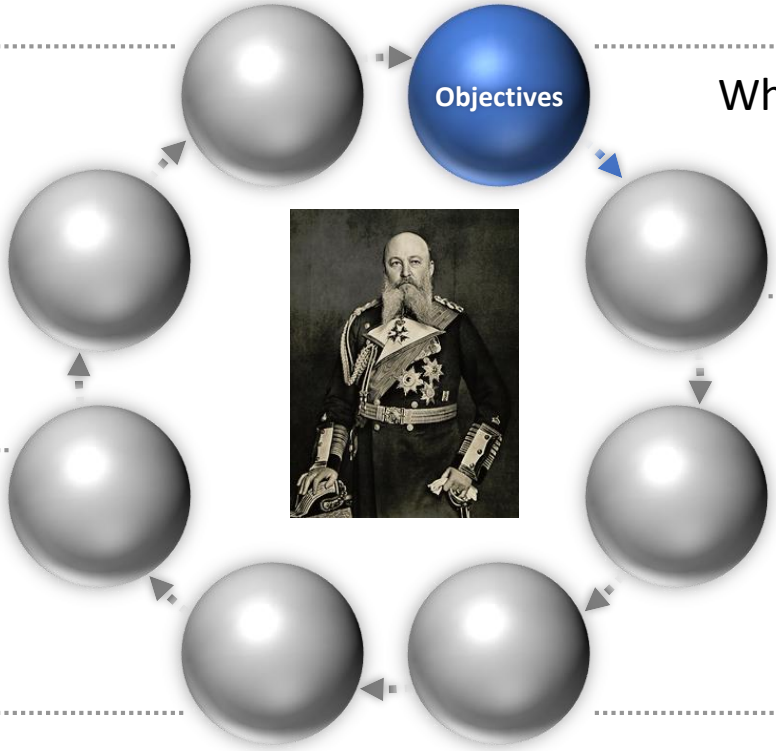
What am I trying to achieve?

Inside Admiral Tirpitz…



What am I trying to achieve?

Inside Admiral Tirpitz…

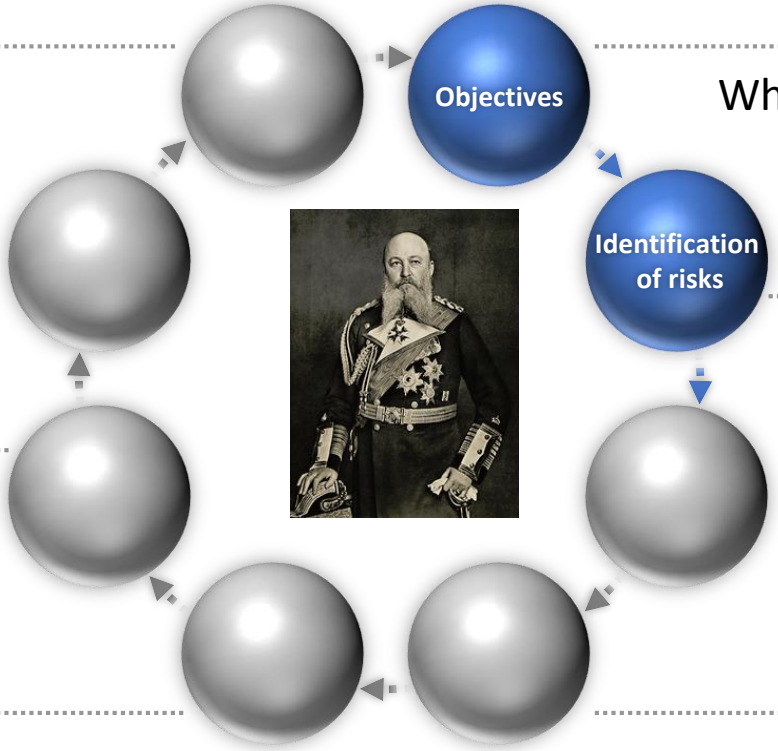


What am I trying to achieve?

What is affecting my objectives?

?

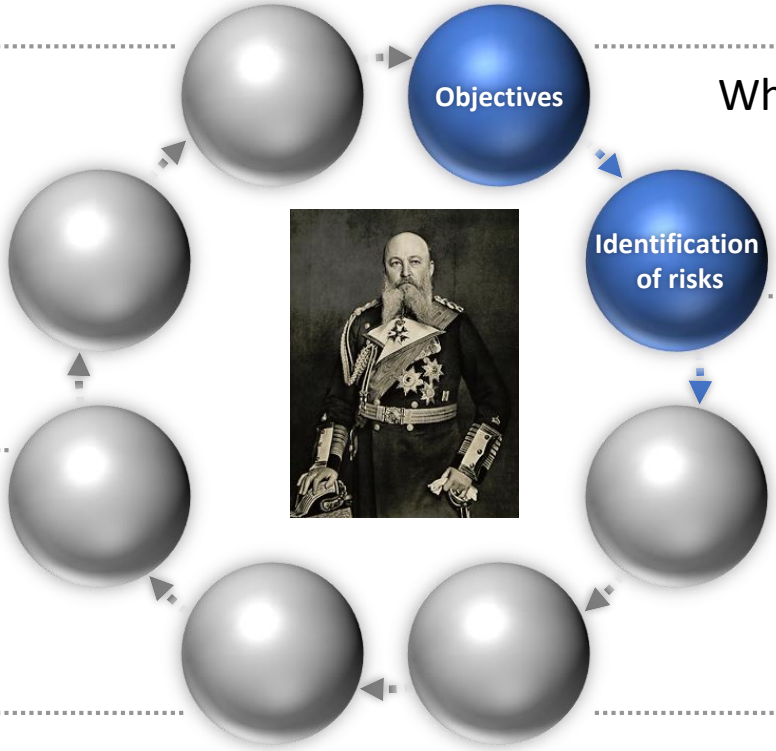
Inside Admiral Tirpitz…



What am I trying to achieve?

What is affecting my objectives?

Inside Admiral Tirpitz…

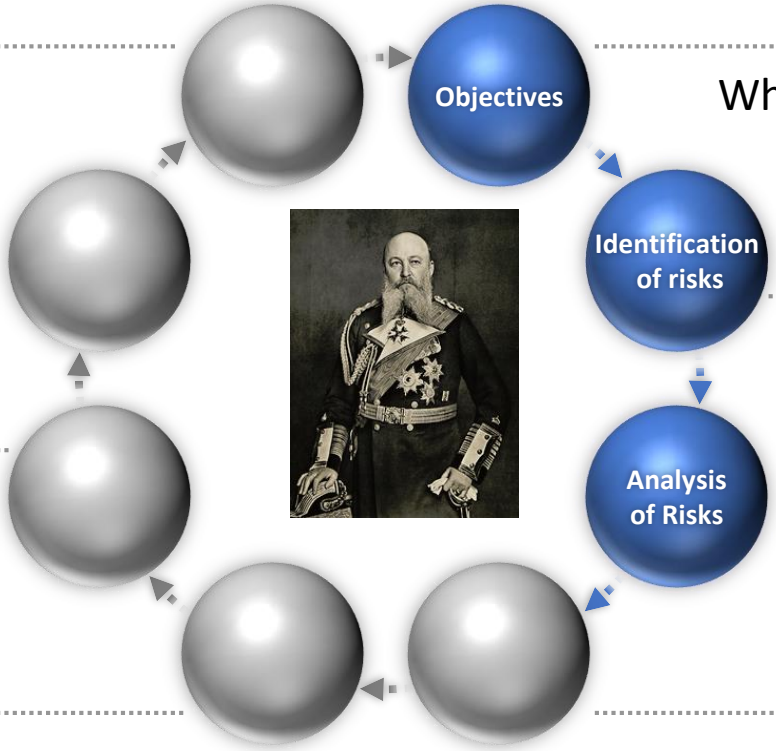


What am I trying to achieve?

What is affecting my objectives?

Which causes and effects exist?

Inside Admiral Tirpitz…

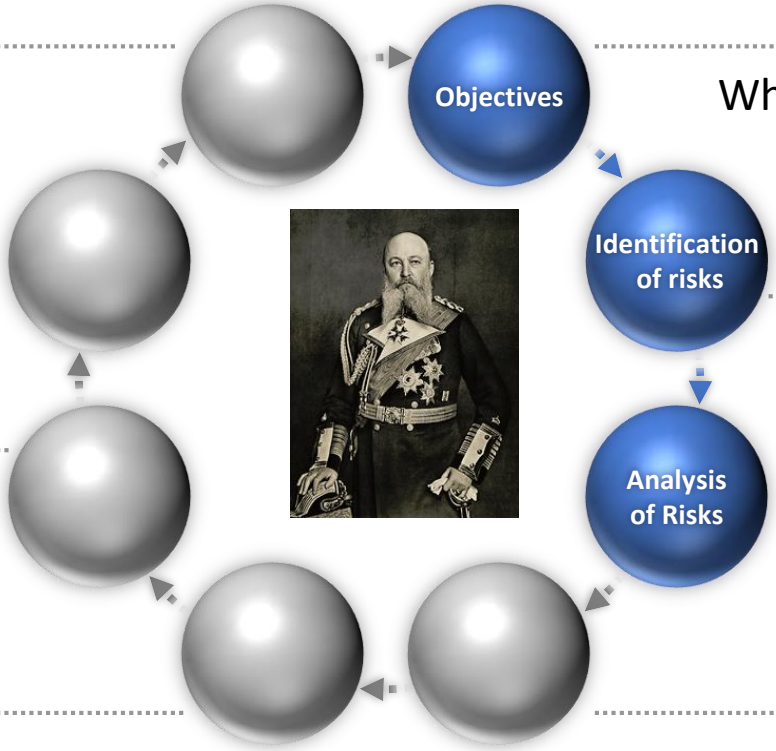


What am I trying to achieve?

What is affecting my objectives?

Which causes and effects exist?

Inside Admiral Tirpitz…



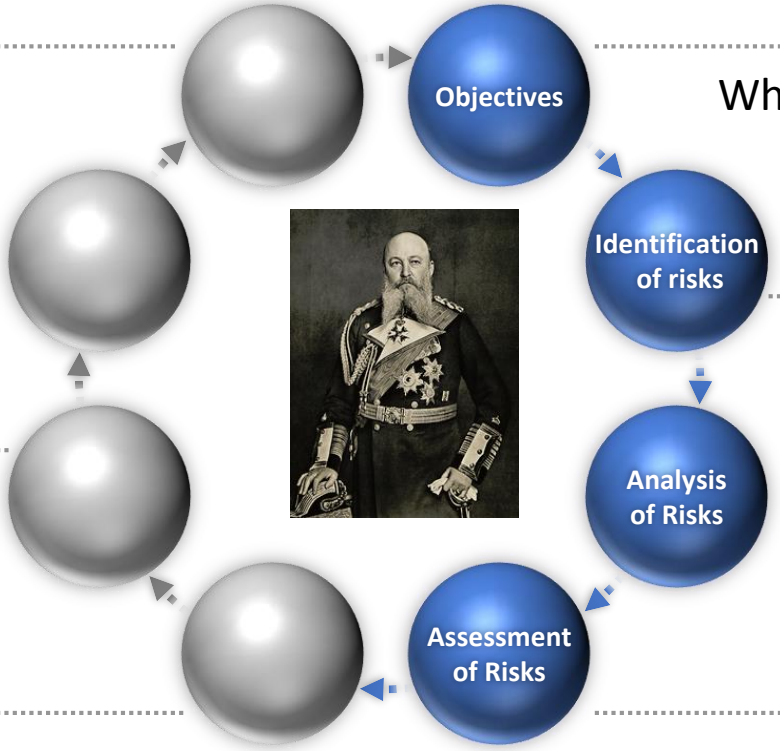
What am I trying to achieve?

What is affecting my objectives?

Which causes and effects exist?

Which are the big ones?

Inside Admiral Tirpitz…



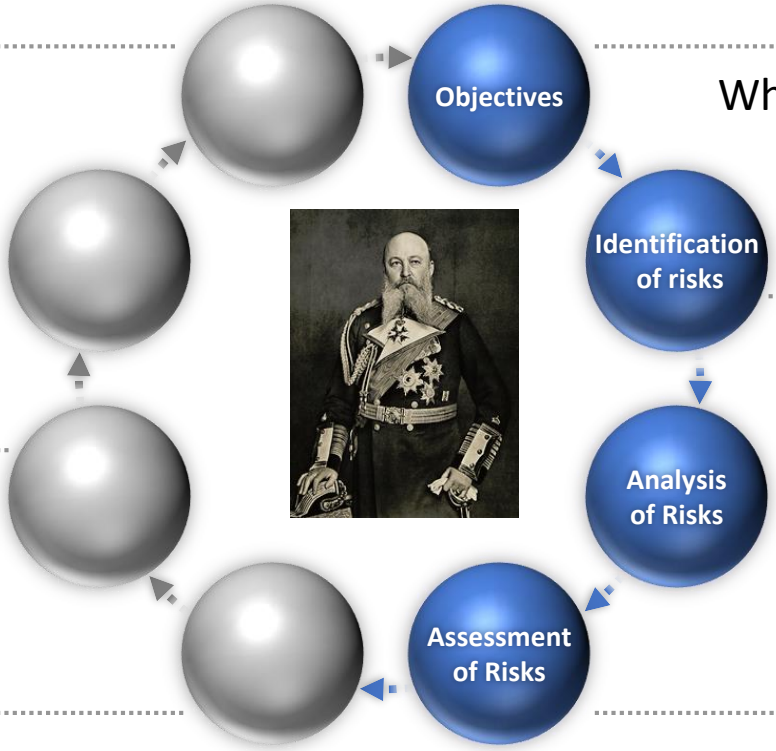
What am I trying to achieve?

What is affecting my objectives?

Which causes and effects exist?

Which are the big ones?

Inside Admiral Tirpitz…



What am I trying to achieve?

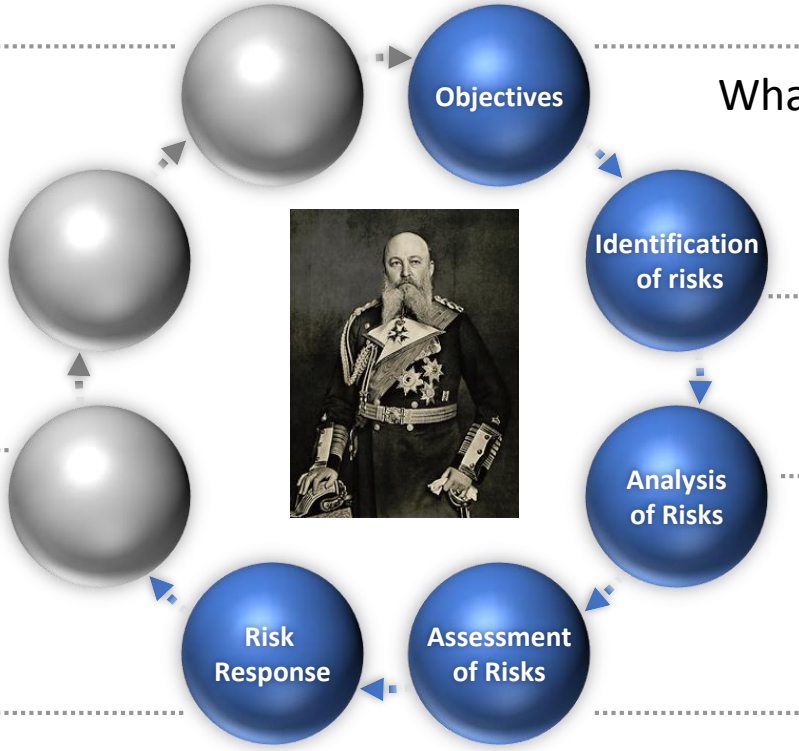
What is affecting my objectives?

Which causes and effects exist?

Which are the big ones?

What can I do about it?

Inside Admiral Tirpitz…



What am I trying to achieve?

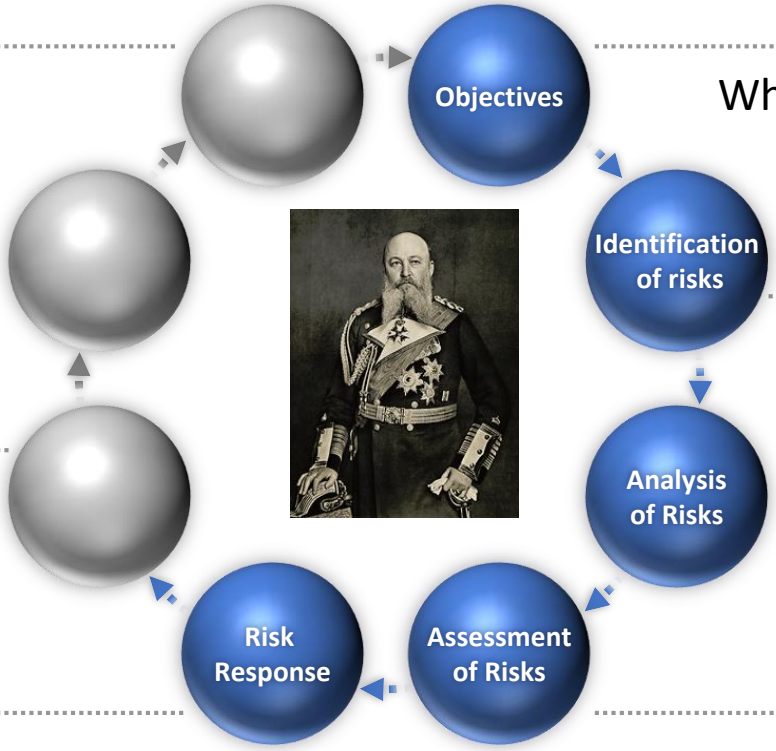
What is affecting my objectives?

Which causes and effects exist?

Which are the big ones?

What can I do about it?

Inside Admiral Tirpitz…



What am I trying to achieve?

What is affecting my objectives?

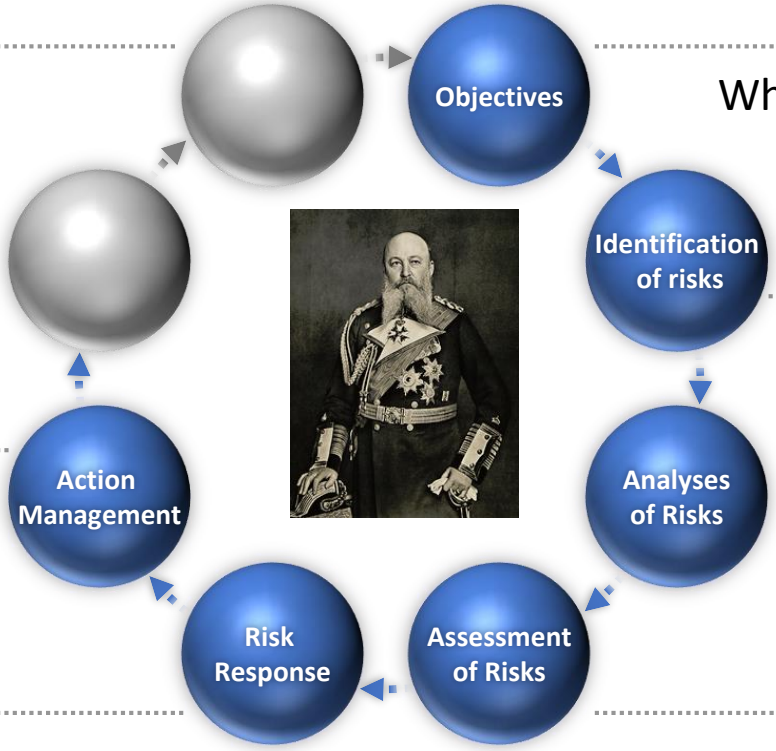
Which causes and effects exist?

Which are the big ones?

What can I do about it?

What are the costs of the implementation vs risk reduction?

Inside Admiral Tirpitz…



What am I trying to achieve?

What is affecting my objectives?

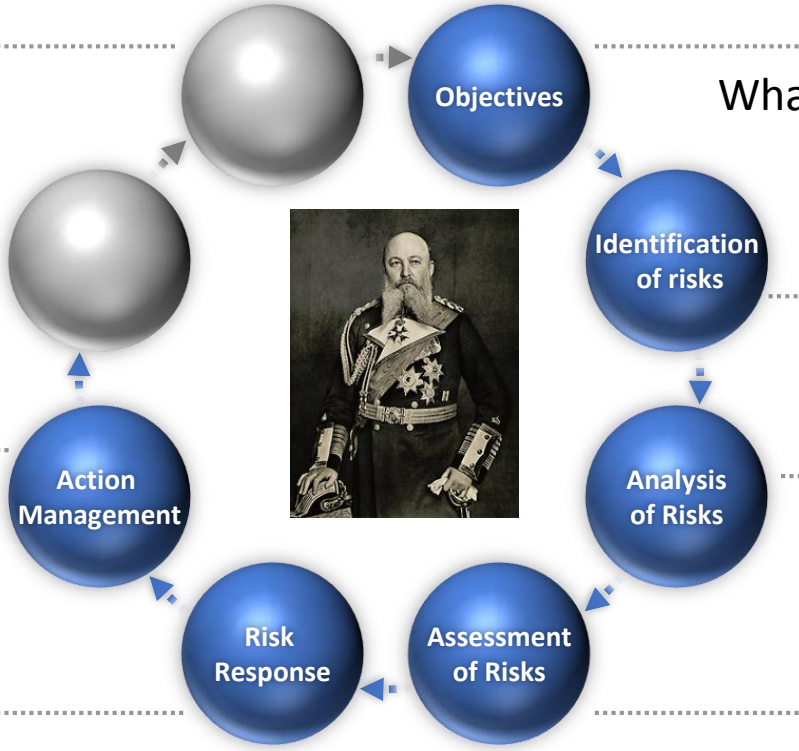
Which causes and effects exist?

Which are the big ones?

What can I do about it?

What are the costs of the implementation vs risk reduction?

Inside Admiral Tirpitz…



What am I trying to achieve?

What is affecting my objectives?

Which causes and effects exist?

Which are the big ones?

What can I do about it?

What are the costs of the implementation vs risk reduction?

What has changed?

Inside Admiral Tirpitz…

Objectives

What am I trying to achieve?

Identification of risks

What is affecting my objectives?

Analysis of Risks

Which causes and effects exist?

Assessment of Risks

Which are the big ones?

Risk Response

What can I do about it?

Action Management

What are the costs of the implementation vs risk reduction?

Risk Review

What has changed?

Inside Admiral Tirpitz…

Who is the target group of my risk report?

What am I trying to achieve?

What has changed?

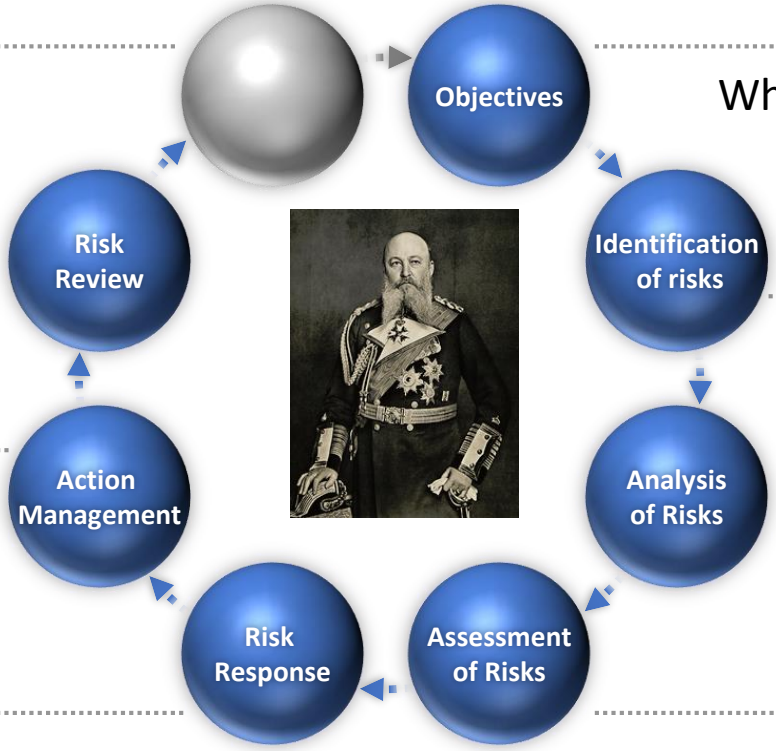
What is affecting my objectives?

What are the costs of the implementation vs risk reduction?

Which causes and effects exist?

What can I do about it?

Which are the big ones?



Inside Admiral Tirpitz…

Who is the target group of my risk report?

What am I trying to achieve?

What has changed?

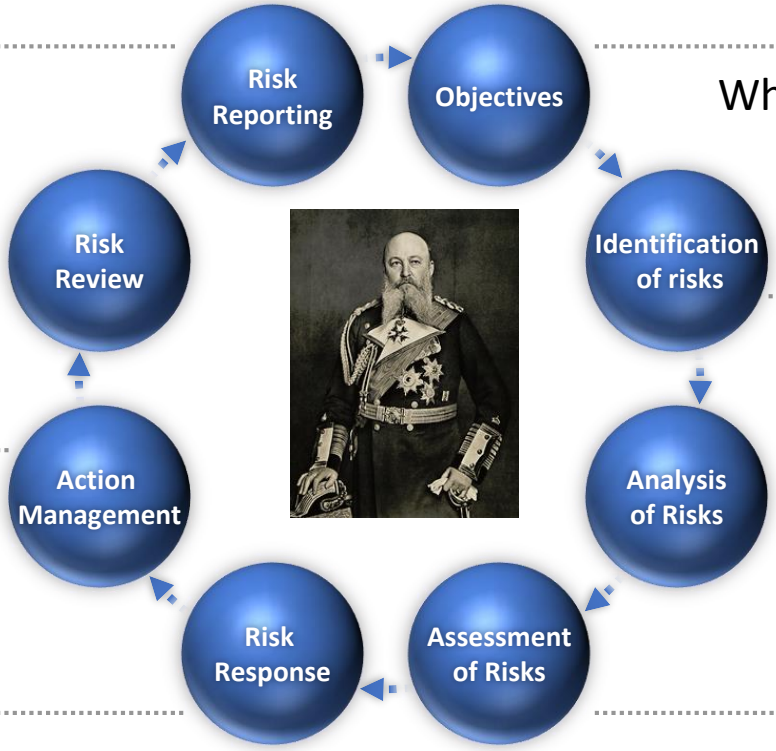
What is affecting my objectives?

What are the costs of the implementation vs risk reduction?

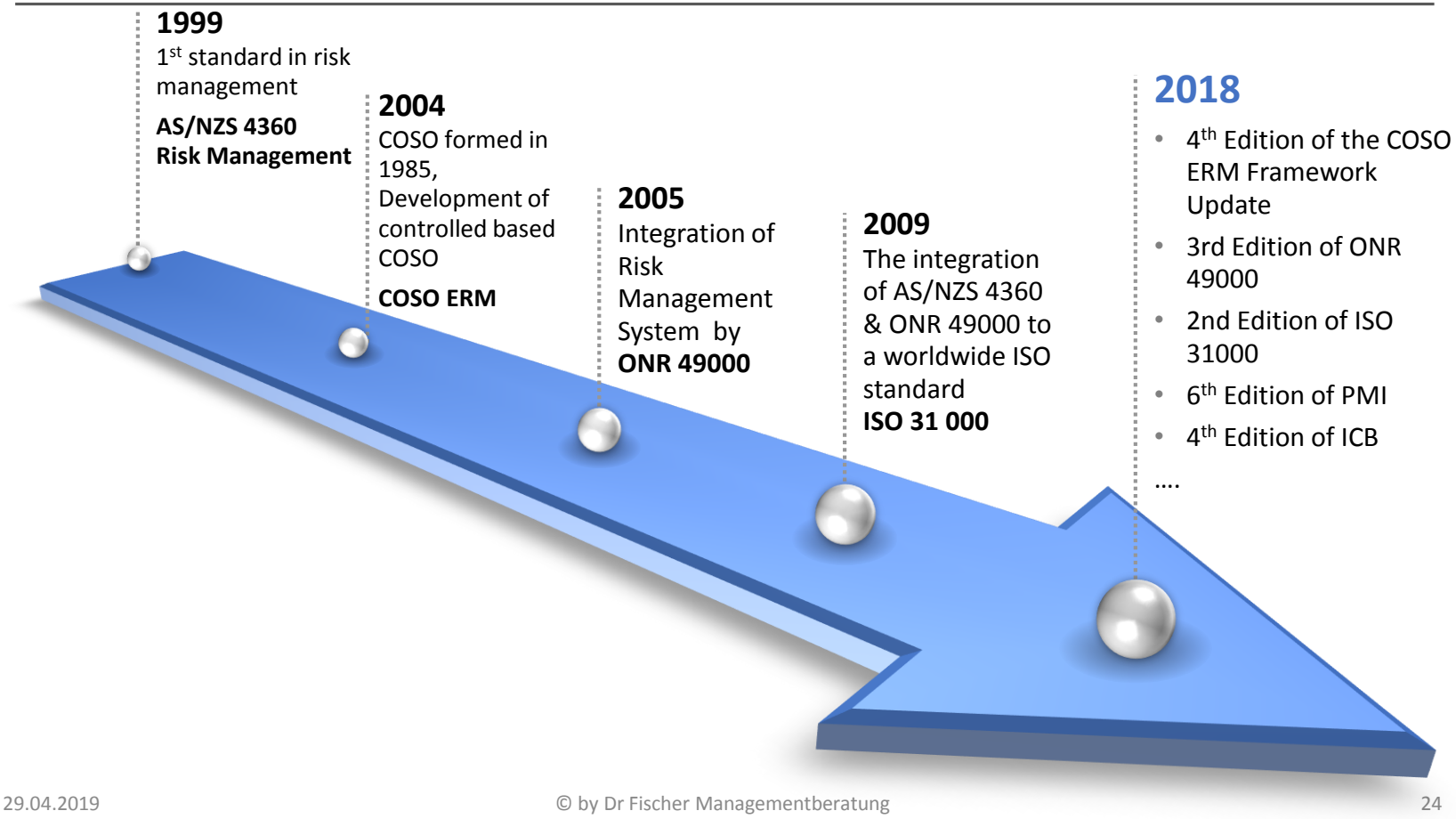
Which causes and effects exist?

What can I do about it?

Which are the big ones?



History of Standardization in Risk Management



What is a Risk?

Risk is an effect of uncertainty on objectives

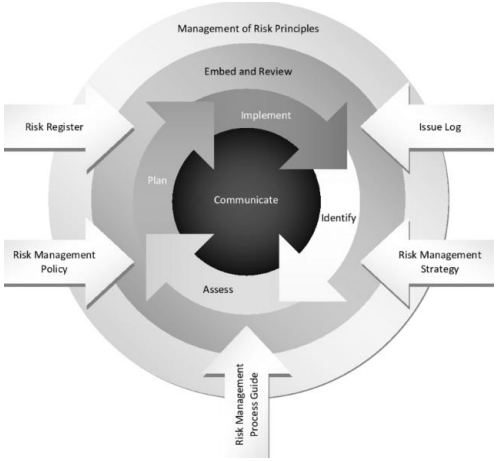
- NOTE 1 An effect is a deviation from the expected — positive and/or negative.
- NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
- NOTE 3 Risk is often characterized by reference to potential **events** and **consequences**, or a combination of these.
- NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** of occurrence
- NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

Definition of ISO 31000

Management of Risk (UK Gvt)

The M_o_R framework is based on four core concepts:

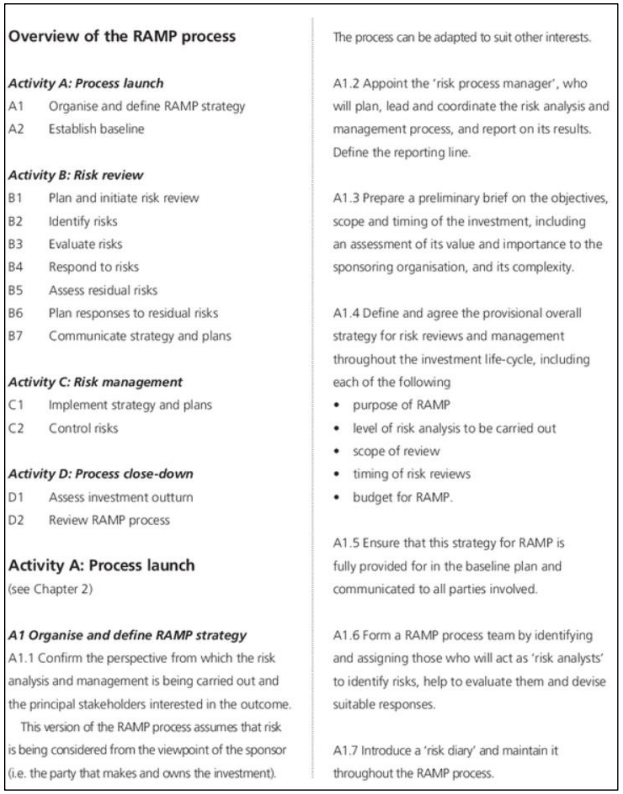
- **M_o_R Principles**. These are essential for the development of good risk management practice. All are derived from corporate governance principles in the recognition that risk management is a subset of any organisation's internal controls.
- **M_o_R Approach**. These principles need to be adapted to suit each individual organisation. Accordingly, an organisation's approach to these principles need to be agreed and defined within a risk management policy, process guide and plans, and supported by the use of risk registers and issue logs.
- **M_o_R Processes**. These six process steps describe the inputs, outputs and activities involved in ensuring that risk are identified, assessed and controlled.
- **Embedding and Reviewing M_o_R**. Having put in place these principles, approaches and processes, for them to be effective, an organisation needs to ensure that they are consistently applied across the organisation and that their application undergoes continual improvement.



https://www.gov.uk/government/publications/management-of-risk-in-government-framework

RAMP-Risk Analysis and Management for Projects

- **RAMP** (Risk Analysis and Management for Projects) is a well-established framework for analyzing and managing the risks involved in projects, whether large or small. With an emphasis on the strategic and financial aspects, this practical working guide will assist planners, engineers, accountants, actuaries, lawyers, project managers, public administrators and anyone else who is involved with a project's success.
- Businesses increasingly need to manage their projects in a turbulent environment, where change is often unexpected and continuous. RAMP's systematic approach helps to ensure that risks are effectively identified, analysed and controlled, and that newly emerging risks can be spotted while there is still time to do something about them.



Overview of the RAMP process

Activity A: Process launch

A1 Organise and define RAMP strategy
A2 Establish baseline

Activity B: Risk review

B1 Plan and initiate risk review
B2 Identify risks
B3 Evaluate risks
B4 Respond to risks
B5 Assess residual risks
B6 Plan responses to residual risks
B7 Communicate strategy and plans

Activity C: Risk management

C1 Implement strategy and plans
C2 Control risks

Activity D: Process close-down

D1 Assess investment outturn
D2 Review RAMP process

Activity A: Process launch

(see Chapter 2)

A1 Organise and define RAMP strategy

A1.1 Confirm the perspective from which the risk analysis and management is being carried out and the principal stakeholders interested in the outcome.

This version of the RAMP process assumes that risk is being considered from the viewpoint of the sponsor (i.e. the party that makes and owns the investment).

The process can be adapted to suit other interests.

A1.2 Appoint the 'risk process manager', who will plan, lead and coordinate the risk analysis and management process, and report on its results. Define the reporting line.

A1.3 Prepare a preliminary brief on the objectives, scope and timing of the investment, including an assessment of its value and importance to the sponsoring organisation, and its complexity.

A1.4 Define and agree the provisional overall strategy for risk reviews and management throughout the investment life-cycle, including each of the following

- purpose of RAMP
- level of risk analysis to be carried out
- scope of review
- timing of risk reviews
- budget for RAMP.

A1.5 Ensure that this strategy for RAMP is fully provided for in the baseline plan and communicated to all parties involved.

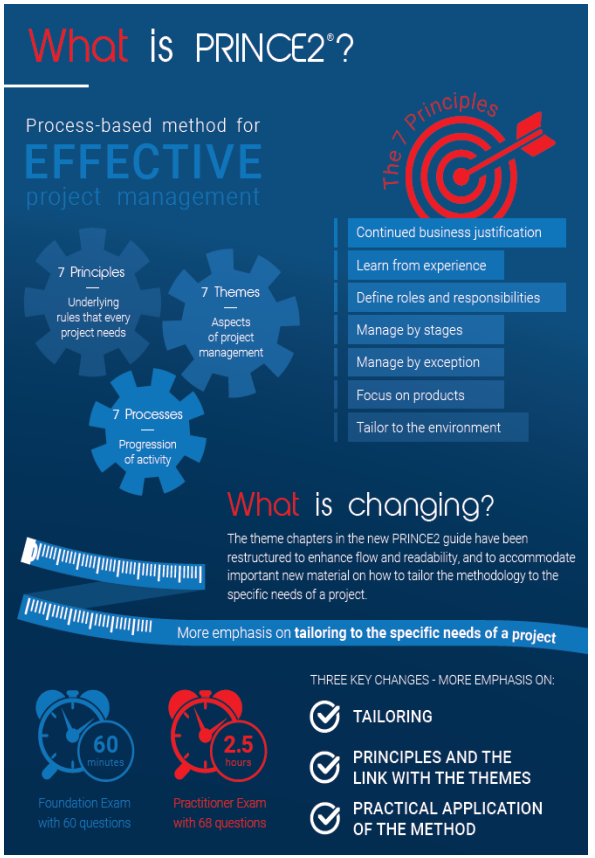
A1.6 Form a RAMP process team by identifying and assigning those who will act as 'risk analysts' to identify risks, help to evaluate them and devise suitable responses.

A1.7 Introduce a 'risk diary' and maintain it throughout the RAMP process.

https://www.ice.org.uk/knowledge-and-resources/best-practice/risk-analysis-and-management-for-projects

PRINCE2-PRojects IN Controlled Environments (UK)

- PRINCE2 (an acronym for **PR**ojects **IN C**ontrolled **E**nvironments) is a de facto process-based method for effective project management.
- PRINCE was originally based on PROMPT, a project management method created by Simpact Systems Ltd in 1975, and adopted by CCTA in 1979 as the standard to be used for all Government information system projects.
- When PRINCE was launched in 1989, it effectively superseded PROMPT within Government projects. PRINCE remains in the public domain and copyright is retained by the Crown.
- PRINCE2 was published in 1996, having been contributed to by a consortium of some 150 European organizations.



https://www.prince2.com/uk/what-is-prince2

PMI – Project Management Institute (US)

- In the 1960s project management as such began to be used in the US aerospace, construction and defense industries.
- The Project Management Institute was founded by Ned Engman (McDonnel Douglas Automation), James Snyder and Susan Gallagher (SmithKline & French Laboratories), Eric Jenett (Brown & Root) and J Gordon Davis (Georgia Institute of Technology) at the Georgia Institute of Technology in 1969 as a nonprofit organization
- "*Risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives*."
- This definition in "real life" is usually an event that has a potential negative effect, but the risk definition in PMI is wider: it includes positive effects as well, called an "opportunity".

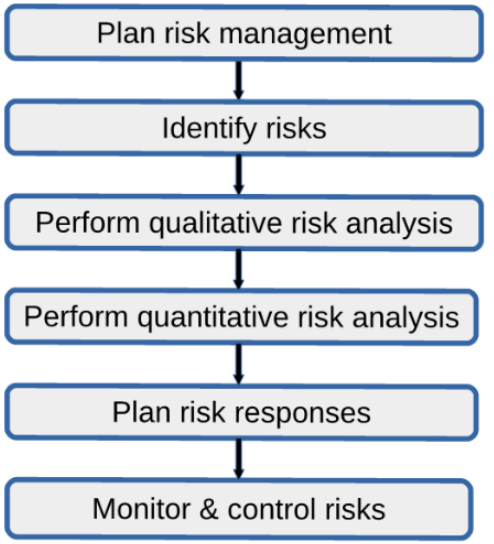


Fig. 1: PMBOK® risk management processes

https://www.pmi.org/certifications/types/risk-management-rmp

A Guide to the Project Management Body of Knowledge (PMBOK® Guide)— 6th Edition (PMI, 2017)

IPMA Int. Project Mgmt Association (EU, Pac Asia)

Individual Competence Baseline (ICB4)

4.5.11. Risk and opportunity

Definition

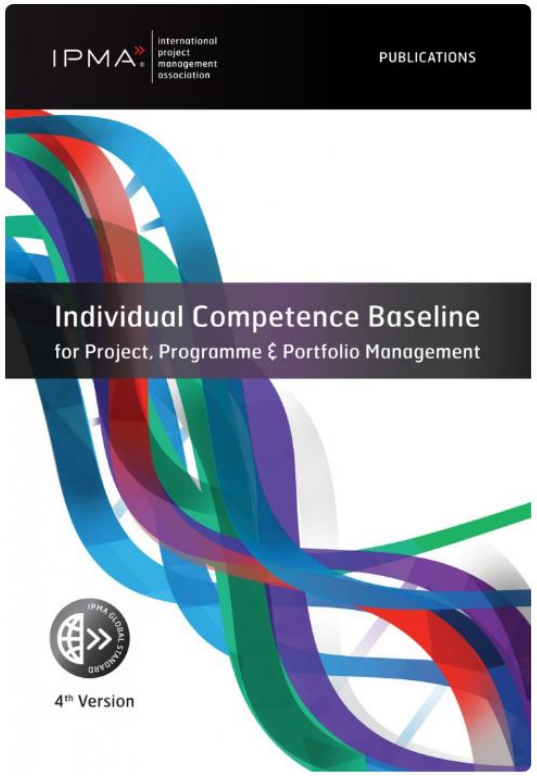
Risk and opportunity includes the identification, assessment, response planning and implementation and control of risks and opportunities around projects. Risk and opportunity management helps decision-makers to make informed choices, prioritise actions and distinguish among alternative courses of action. Risk and opportunity management is an ongoing processtaking place throughout the lifecycle of the project.

Purpose

The purpose of this competence element is to enable the individual to understand and effectively handle risks and opportunities, including responses and overall strategies.

Description

Risk (negative effects) and opportunity (positive effects) are always viewed in their relation to and consequences for realising the objectives of the project. It is advisable as a first step to consider which overall strategies would best serve the handling of risks and opportunities relative to the corporate strategies and the project in question. After that, the risk and opportunity management process is characterised by first identifying and assessing risks and opportunities, followed by the development and implementation of a response plan covering the intended and planned actions for dealing with identified risks and opportunities. The response plan should be developed and implemented in line with the chosen overall risk and opportunity strategies. The individual is responsible for involving team members and keeping the team committed to the risk and opportunity management process; for making the team alert to risks and opportunities; for involving other stakeholders in the process and for involving the appropriate subject matter experts whenever necessary.



https://www.ipma.world/individuals/standard/

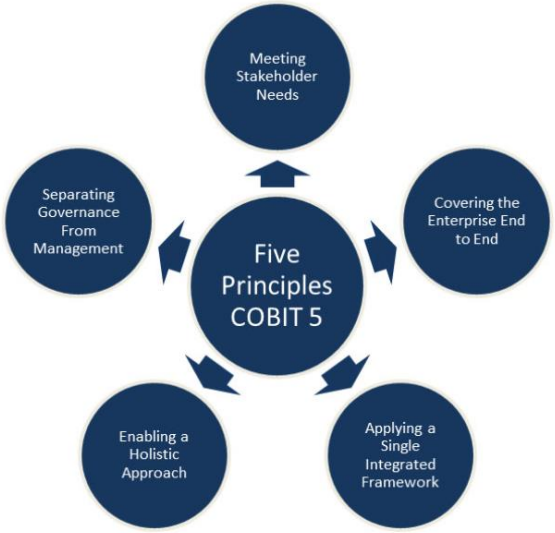
Individual Competence Baseline (ICB4) , 2016

COBIT 5 (**C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology)

- As an independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems.
- Previously known as the **Information Systems Audit and Control Association**, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.
- ISACA got its start in 1967, when a small group of individuals with similar jobs sat down to discuss the need for a centralized source of information and guidance in the field.
- In 1969, the group formalized, incorporating as the EDP Auditors Association. In 1976 the association formed an education foundation to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field.

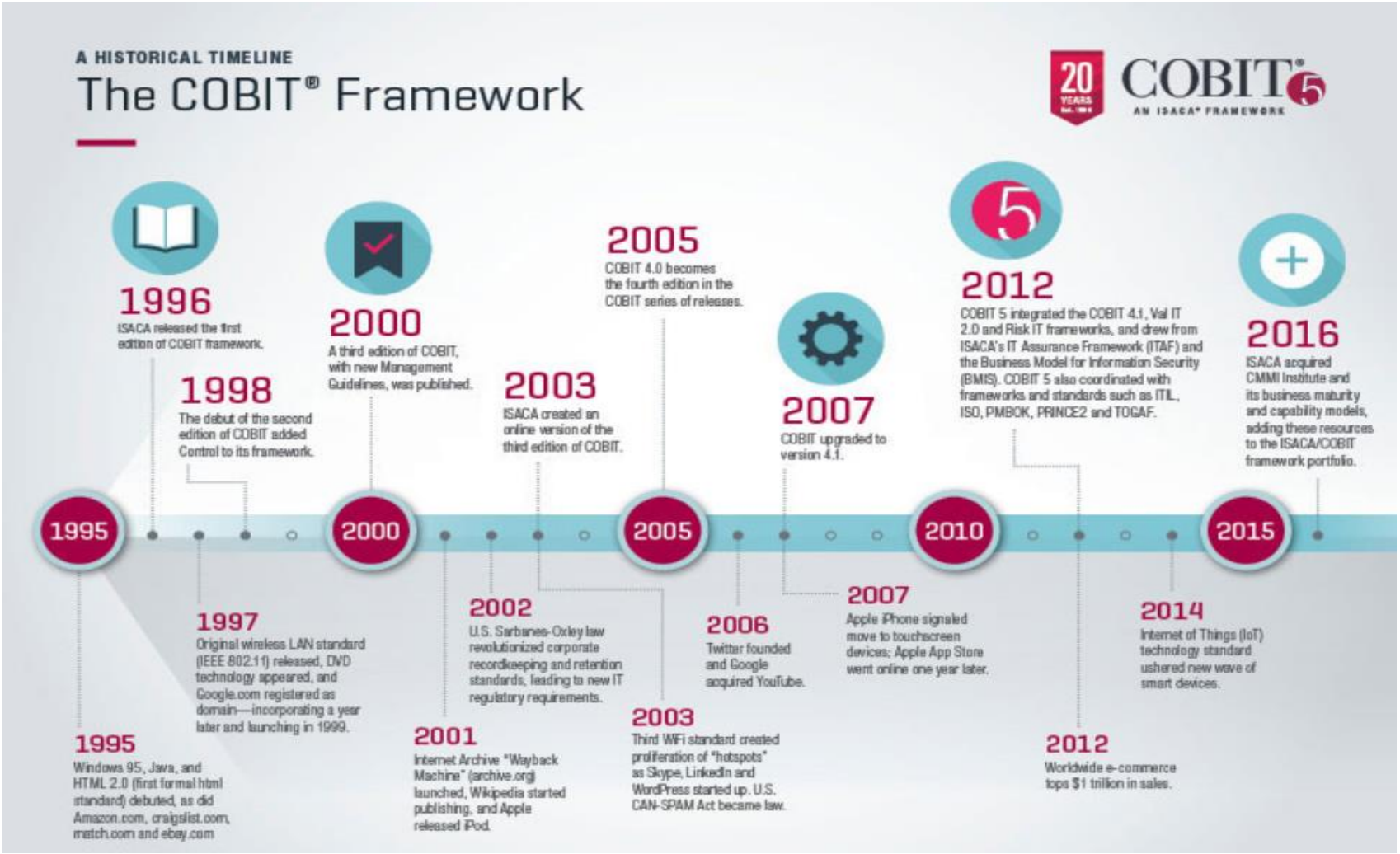
COBIT® 5

AN ISACA® FRAMEWORK



http://www.isaca.org/Knowledge-Center/Academia/Pages/risk-management.aspx

COBIT 5



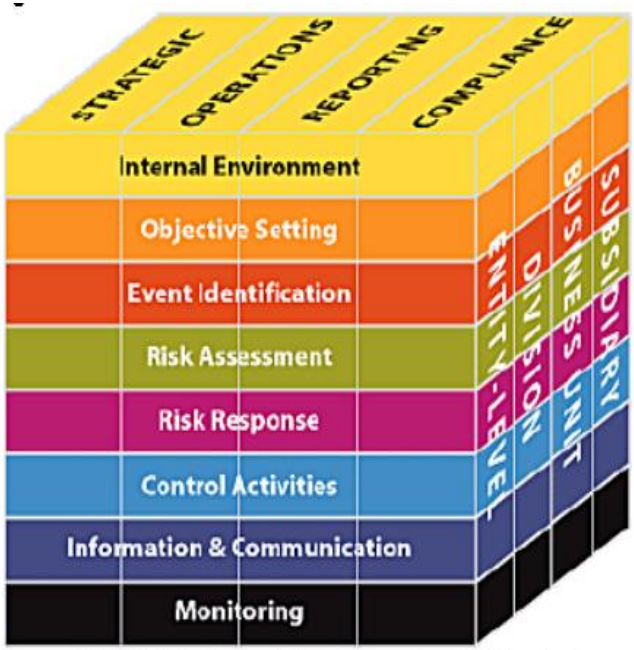
COSO II ERM Framework

- COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (Treadway Commission)
- The Treadway Commission was originally jointly sponsored and funded by five main professional accounting associations and institutes headquartered in the United States
- These five organizations formed what is now called the Committee of Sponsoring Organizations of the Treadway Commission. (COSO)

COSO II ERM Framework

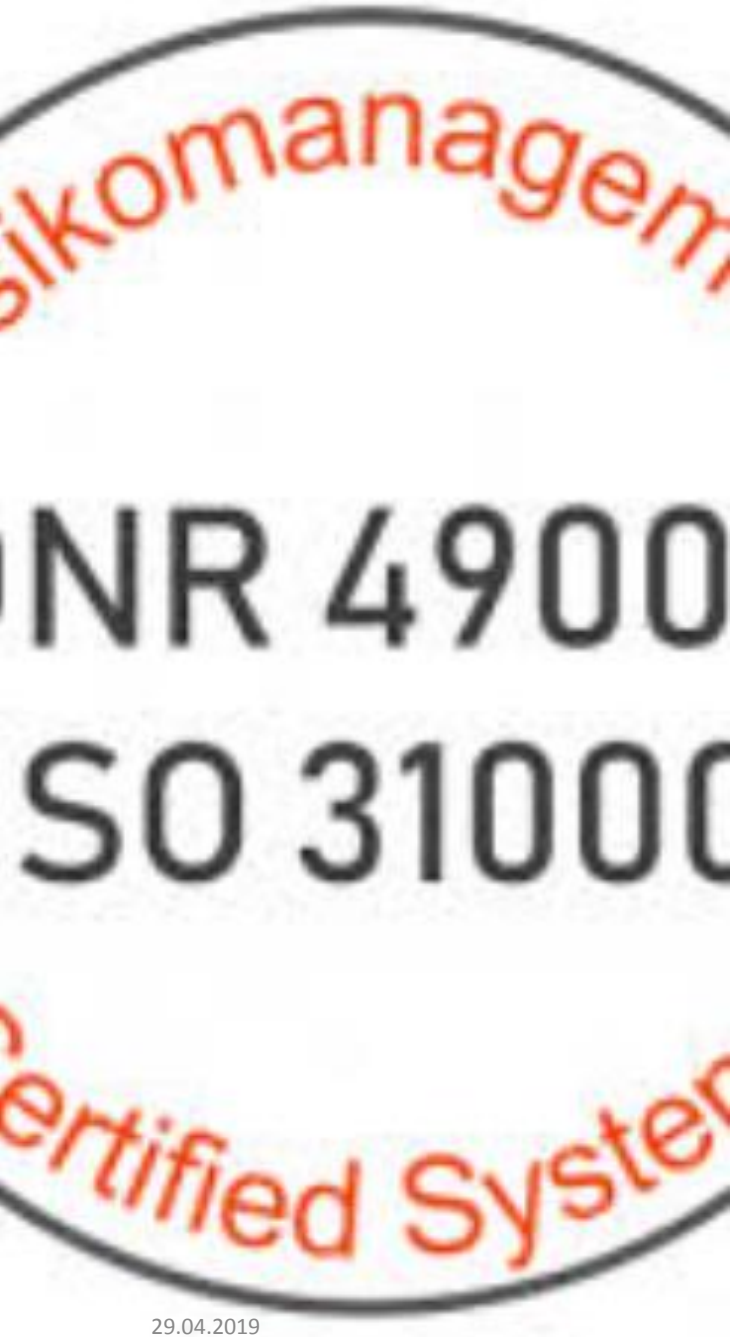
COSO II - Enterprise Risk Management Integrated Framework (2004), defines essential components, suggests a common language, and provides direction and guidance for ERM.

- Notably, ERM requires an entity to take a view of risk that examines the entire organization, from the enterprise level, to a division or subsidiary, to the level of a single business units processes.
- As shown in Figure 1, ERM consists of eight interrelated components, which are integral to the way management runs the enterprise. The components are linked and serve as criteria for determining whether ERM is effective.
- Internal control is encompassed within, and is an integral part of, ERM.
- ERM is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk.



Source: COSO ERM Integrated Framework, dated September 2004

https://www.coso.org/Pages/erm-integratedframework.aspx



ONR 4900x:2014

By issuing the ONR series 4900x:2014 “Risk management for organizations and systems”, Austrian Standards publishes a body of rules supporting the implementation of the International Standard ISO 31000 “Riskmanagement — Principles and guidelines”

The standard consists of 6 parts:

- ONR 49000: Terms and Basics
- ONR 49001: Risk Management
- ONR 49002-1: Guidelines
- ONR 49002-2: Guidelines
- ONR 49002-3: Guidelines
- ONR 49003: Qualification of a Risk Manager

https://shop.austrian-standards.at/action/de/public/details/514131/ONR_49000_2014_01_01

ONR 49000:2014

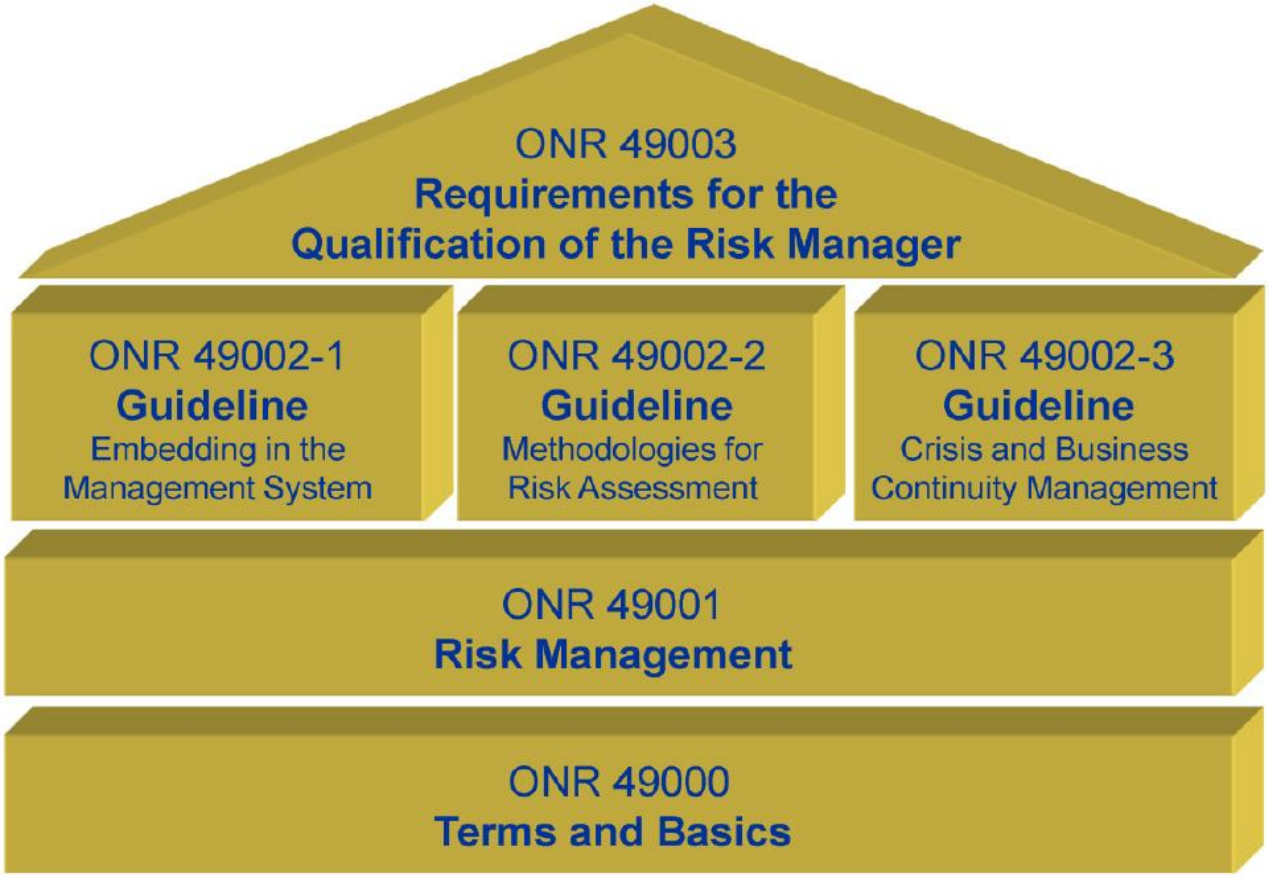


Figure 1 — Risk management for organizations and systems

ONR 49000:2014

Figure 4— Risk management system

ONR 49000:2014

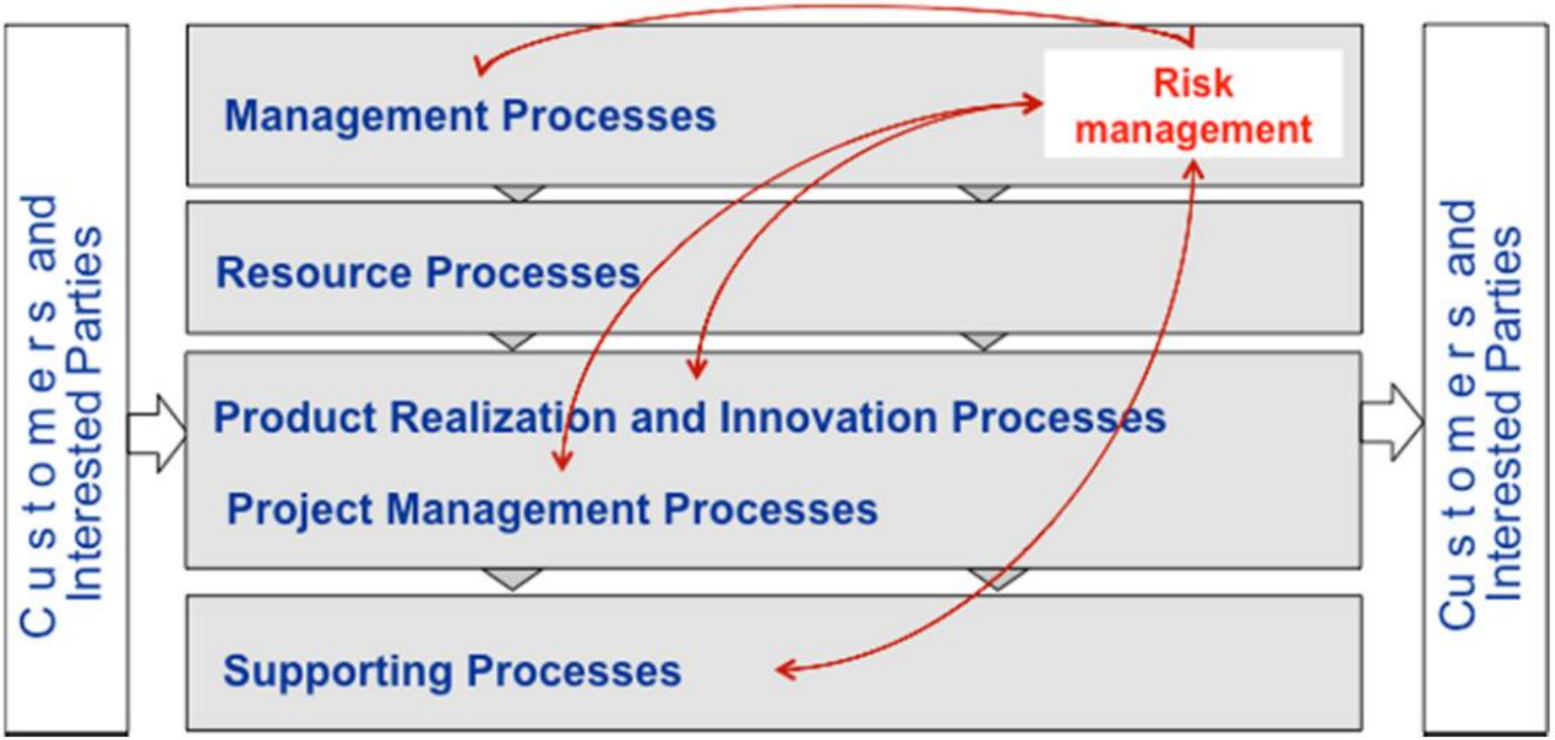


Figure 4 — Risk Management in the existing process flows

ONR 49000:2014

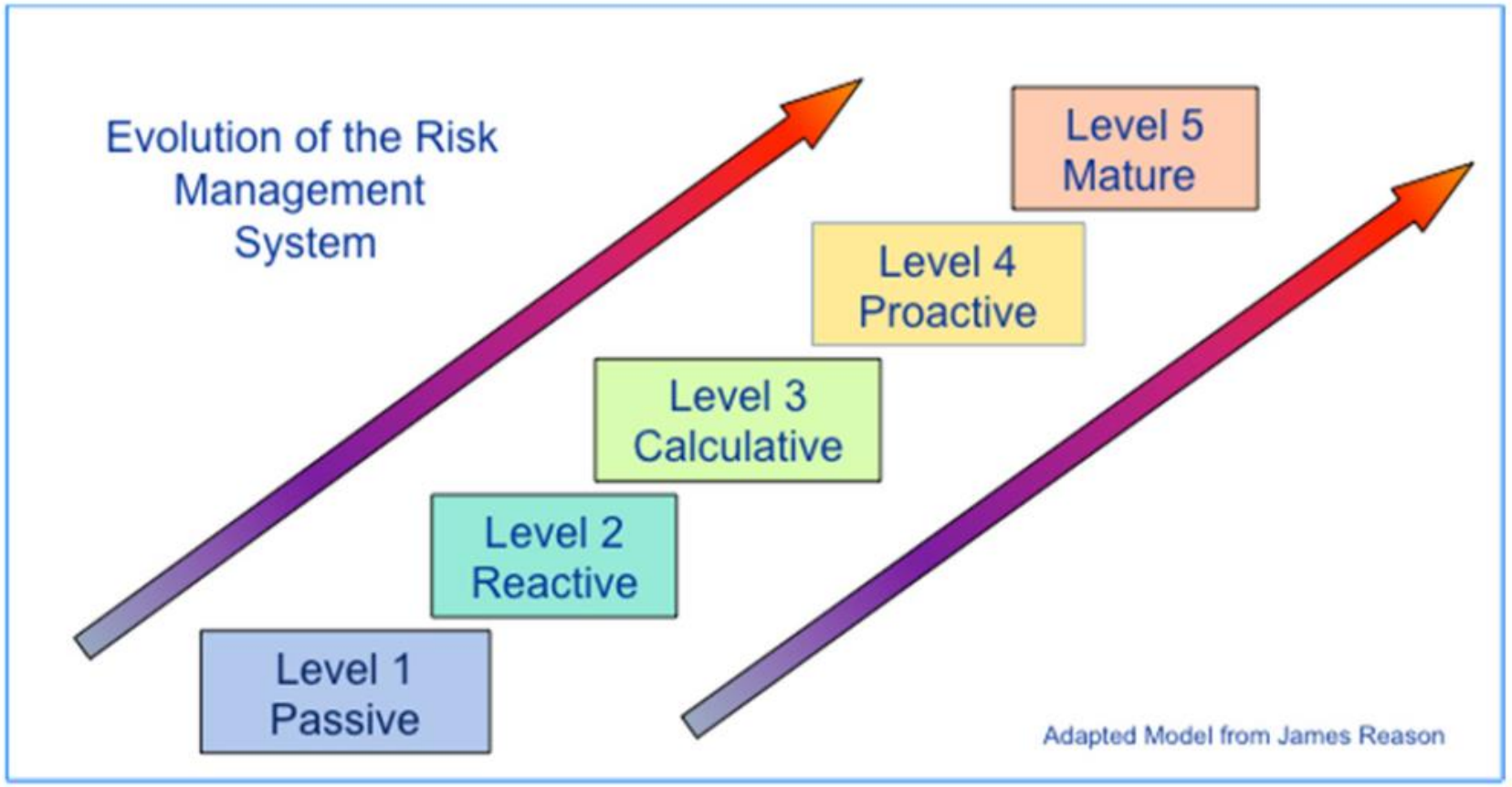


Figure 6 — Development of the risk management system

ONR 49000:2014

	Risk 1	Risk 2	Risk 3	Risk 4
Risk 1		-	0	-
Risk 2	-		++	+
Risk 3	0	++		0
Risk 4	-	+	0	

Explanation:
0 no interdependency
\+ risks reinforce each other
\- risks offset each other

Figure 9a

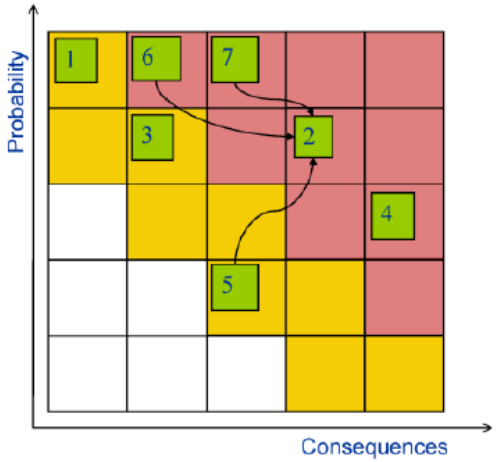


Figure 9b

Figure 9 — Interdependencies of risks (example)

ONR 49000:2014

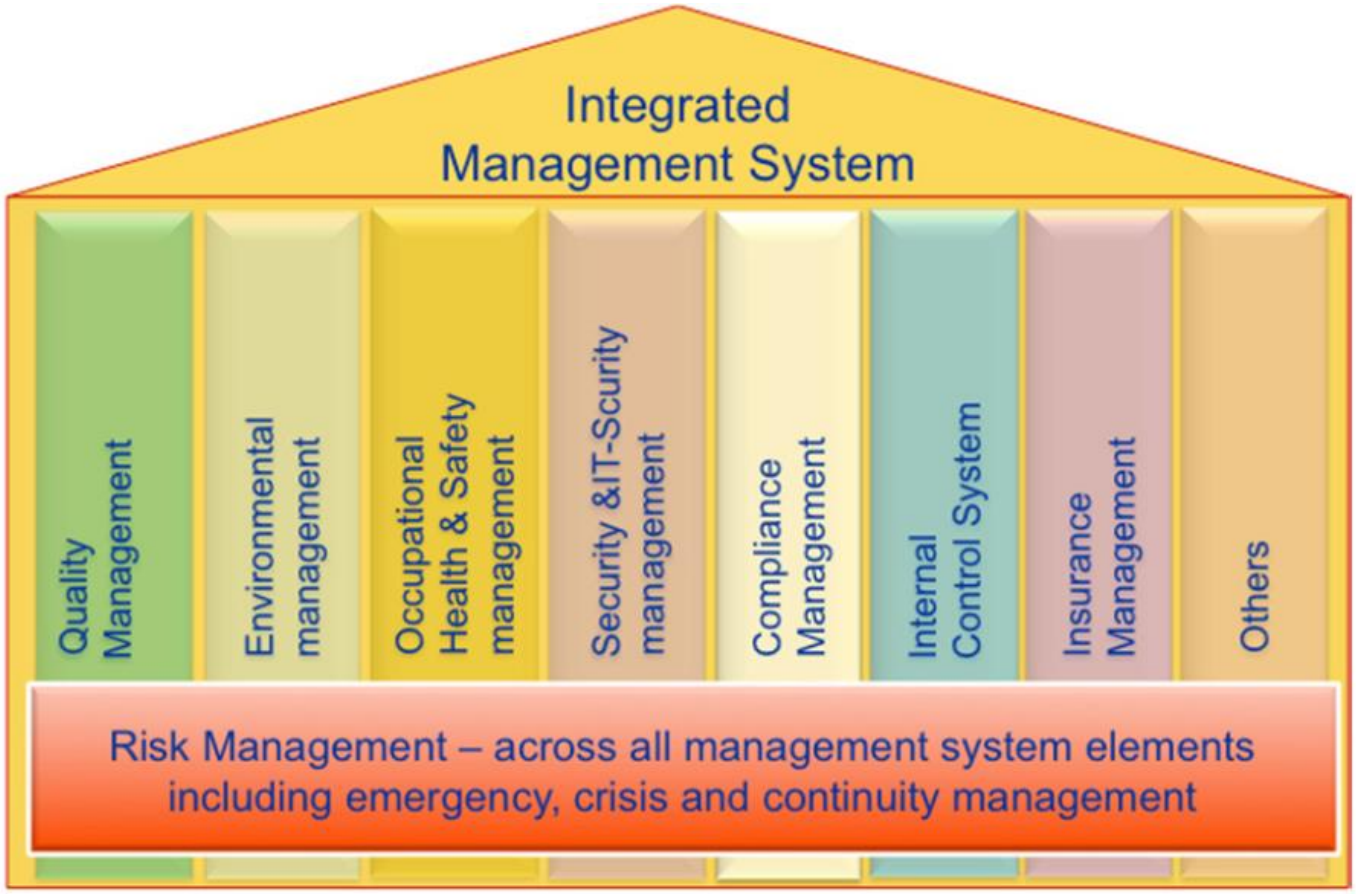


Figure 7 — Links of risk management with other subsystems

ONR 49000:2014

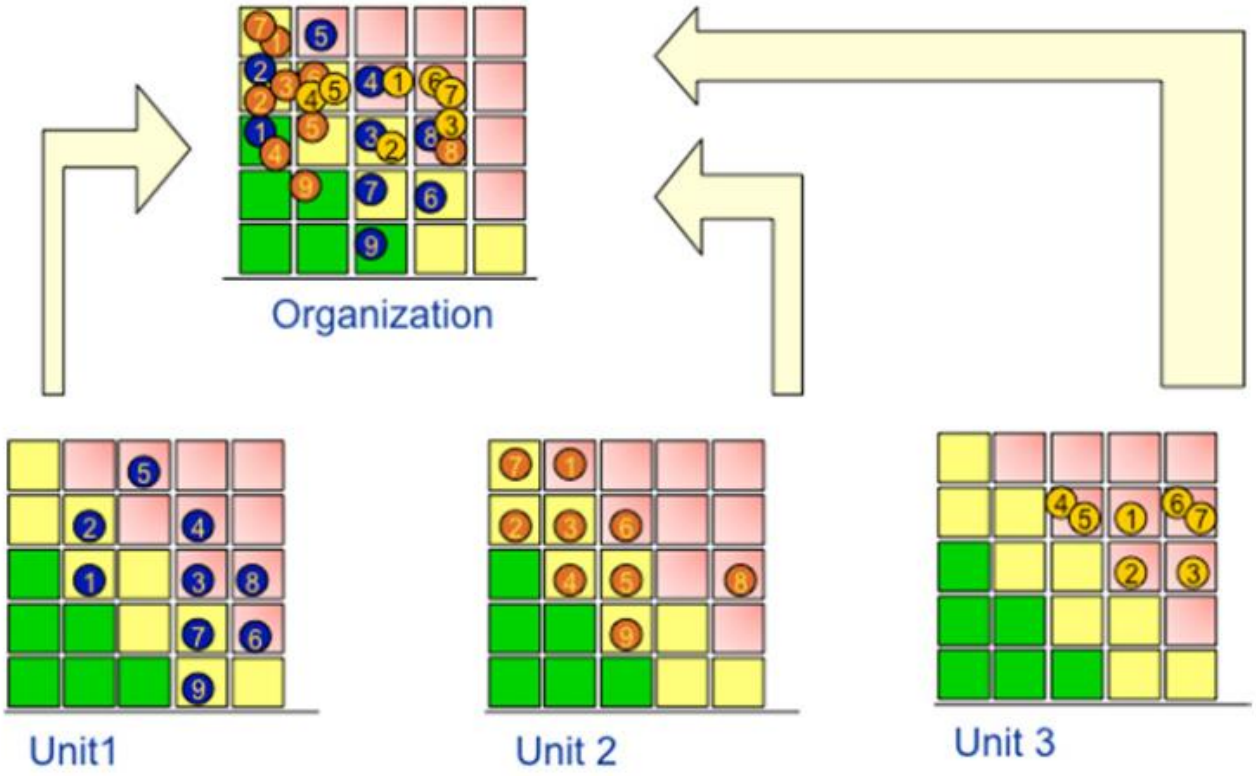


Figure 9 — Consolidation of risks in the organization

ONR 49000:2014

Table 1 — Overview of methods used in the risk management process

Risk management process					
Method	Identification	Assessment			Treatment
		Consequences	Likelihood	Level of risk	
Brainstorming	+++	+	+		+
Delphi method	++	++	++		++
World Café	+++	+	+		
Citizens Conference	+++	++	+		+
Root Cause analyses	++	+	+		+++
London Protocol	+++	+			+++
Fault tree and event tree analysis		++	+++	+	+
Scenario analysis	+++	+++	++	++	+++
CIRS (critical incident reporting system)	+++		+		++
CBRM (change-based risk management)	+++	+		++	
FMEA (failure mode and effects analysis)	+++	++	++	+	+++
Hazard analysis	++	+++	++	++	+++
HAZOP (hazard and operability study)	+++	+++	++	+	+++
HACCP (hazard analysis and critical control points)	++	++			+++
Standard deviation		++	+++	++	
Confidence interval		++	+++	++	
Monte Carlo simulation	+	++	+++	++	

Explanation:
+ good
++ very good
+++ excellent

ONR 49000:2014

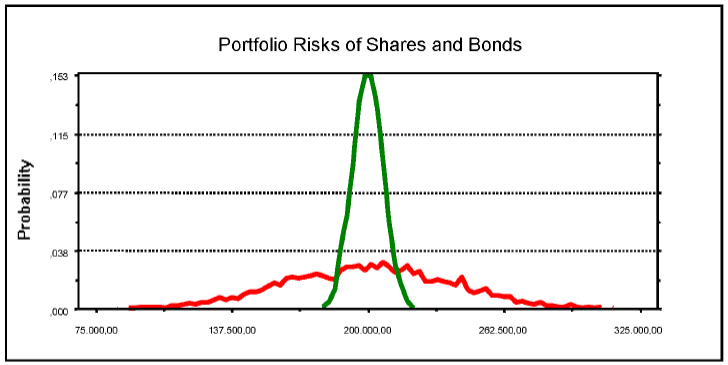


Figure 12 — Standard deviation for different investments (shares and bonds)

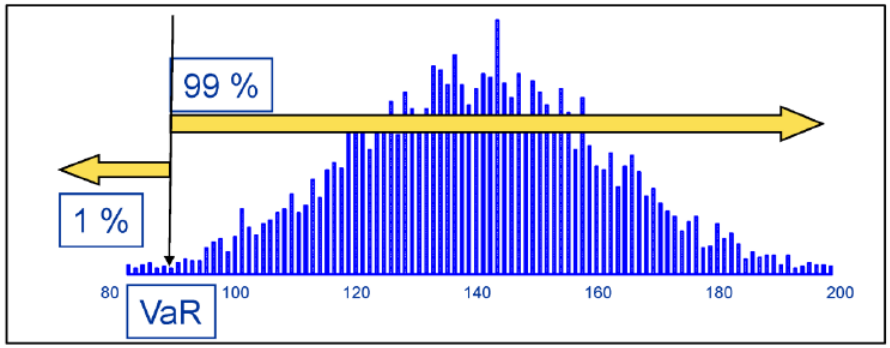
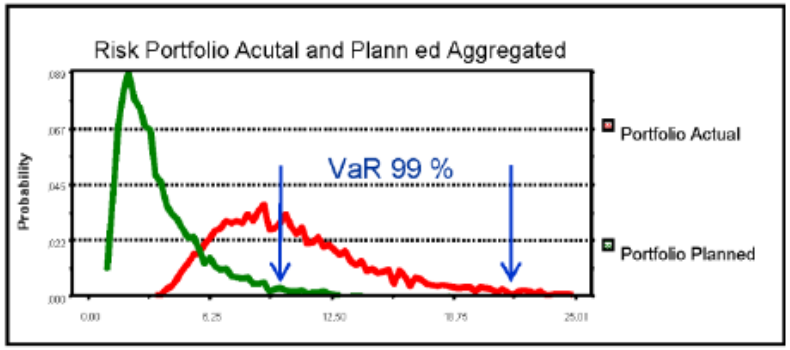


Figure 13 — Confidence interval and value at risk as a measure of risk



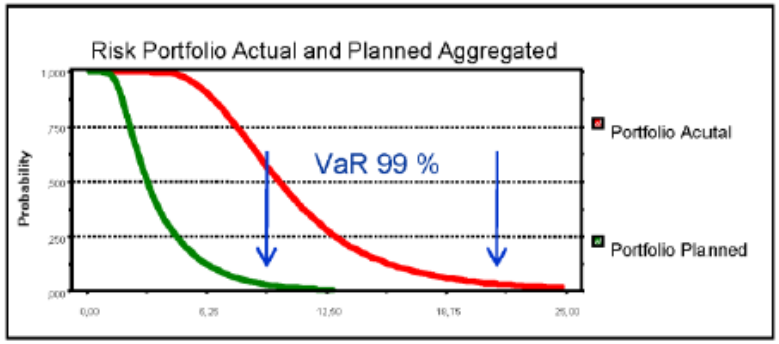


Figure 14 — Confidence interval and value at risk as a measure of risk

ONR 49000:2014

Table A.1 — General risk criteria for consequences

Stage	General, Performance	Injuries to persons	Loss of reputation and assets	Finances
Negligible	In view of the organization's size, the risk is negligible; customers are barely affected .	Minor injuries to persons not resulting in any absence from work.	It causes sporadic complaints and criticism	The financial loss is barely perceptible in the budget
Marginal	The risk causing disturbances and additional costs, individual customers are dissatisfied.	Curable injuries to persons resulting in absence from work.	Media coverage with criticism lead to public emotions against the activities, products, services.	The financial loss leads to budget deviations.
Significant	The risk affects production of goods and services. Individual operating functions are affected and caused serious delivery delays.	Injuries with mild permanent health damage; the quality of life is only affected to a minor extent (bodily injury).	Criminal investigations have been initiated; prosecutions for failure, gross negligence or violations of laws and values.	The financial result is perceptibly affected; profit and liquidity are noticeably affected.
Critical	Organization's capabilities are affected, and customer losses increase.	Severe permanent health damage; quality of life is heavily reduced.	Criminal investigations lead to long-term and regional loss of confidence, which is reparable only with great effort.	The financial result is adversely affected; the damage rises to the level of annual profit. The liquidity is tight.
Catastrophic	The whole organization is affected by the risk; the market position is lost. The continuation of the organization is called into question.	Personal injury resulting in death or severe disability with long term effects	Serious violations of safety regulations and public perception force the resignation of those responsible. The damage caused is almost irreparable.	The financial consequences of the risk exceed the amount of one annual profit and lead to loss of equity. Threat of insolvency.

ONR 49000:2014

Table A.2 — General risk criteria for the probability of occurrence or frequency (low)

Stage	Frequency
Frequent	Once a year, or more frequently
Possible	Once in three years
Remote	Once in ten years
Occational	Once in thirty years
Improbable	Less than once in thirty years

Table A.3 — General risk criteria for the probability of occurrence or frequency (high)

Stage	Frequency
Frequent	Once a month, or more frequently
Possible	Once per quarter
Remote	Once per years
Occational	Once in three years
Improbable	Less than once in three years

Table A.4 — General risk criteria for probability

Stage	Frequency
Frequent	> 30 % up to 100 %
Possible	> 10 % up to 30 %
Remote	> 3 % up to 10 %
Occational	> 1 % up to 3 %
Improbable	1 % or less

ISO 3100x:2018

- **ISO 31000:2018, *Risk management – Guidelines***, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector.
- Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
- However, ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programmes.
- Organizations using it can compare their risk management practices with an internationally recognised benchmark, providing sound principles for effective management and corporate governance.

ISO 31000:2018

5.2
Mandate and commitment

PLAN

5.3
Framework design for managing risk

ACT

5.6
Continual improvement of the framework

Principles (Clause 4)

5.4
Implementing risk management

DO

CHECK

5.5
Monitoring and review of the framework

Process (Clause 6)

ISO 31000:2018

5.2 Mandate and commitment

PLAN

5.3 Framework design for managing risk

- 5.3.1 Understanding the organization and its environment
- 5.3.2 Risk management policy
- 5.3.3 Integration into organizational processes
- 5.3.4 Accountability
- 5.3.5 Resources
- 5.3.6 and 5.3.7 Establishing internal and external communication and reporting mechanisms

ACT

5.6 Continual improvement of the framework

5.4 Implementing risk management

- 5.4.1 Developing a plan for implementation
- 5.4.2 Implementing the framework
- 5.4.3 Implementing the process

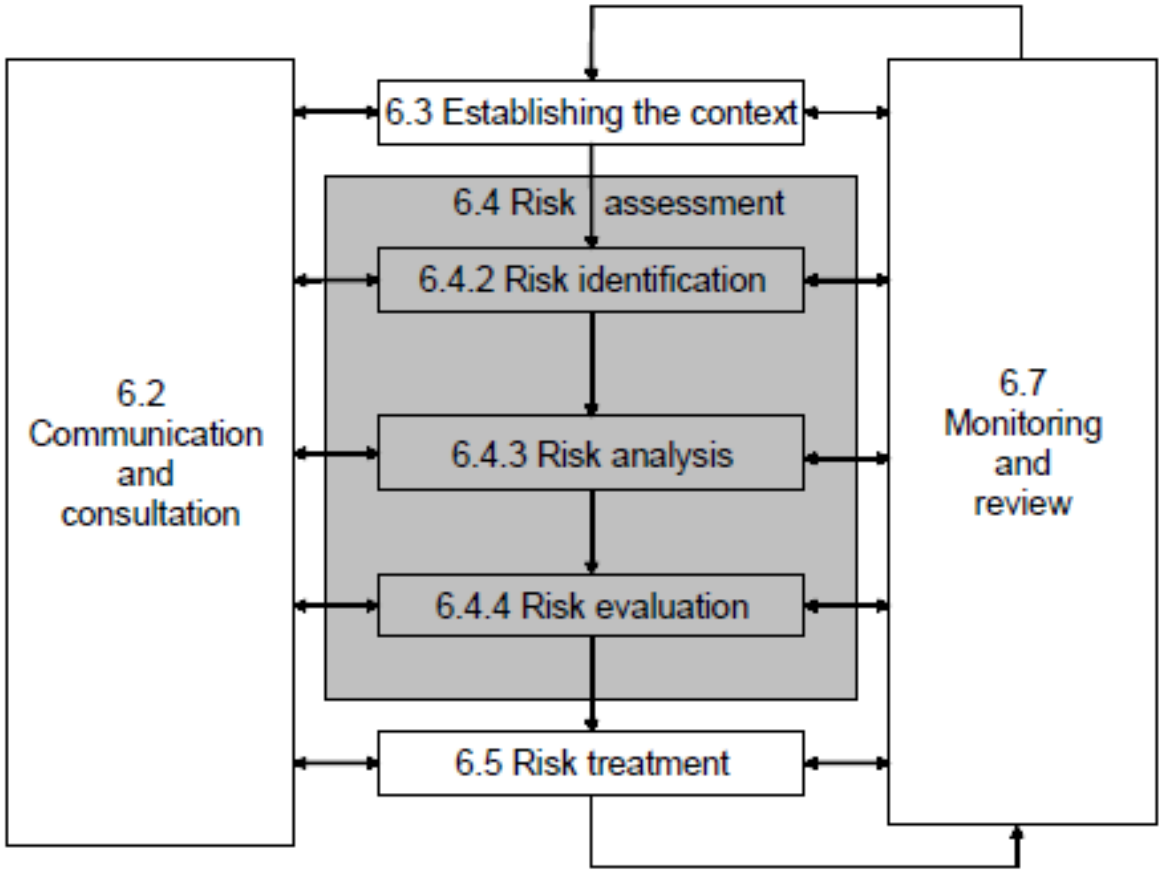
DO

CHECK

5.5 Monitoring and Review of the framework

ISO 31000:2018

DO



ISO 31000:2018

Important attributes of Risk Management System (Plan-Do-Check-Act)

An emphasis is placed on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.

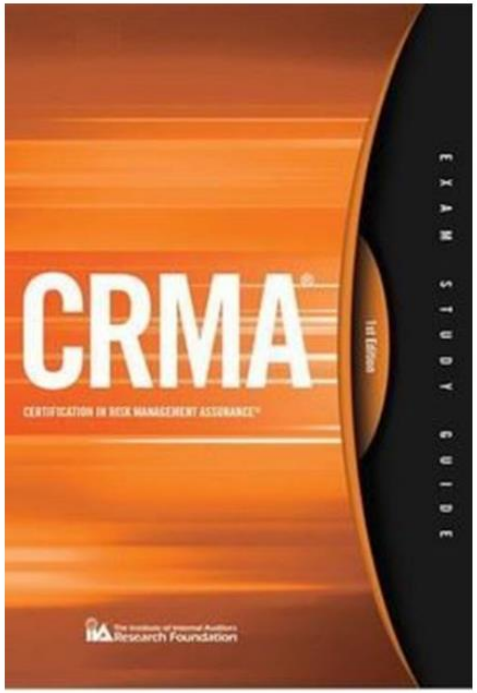
- This can be indicated by the existence of explicit performance goals against which the organization's and individual manager's performance is measured.
- The organization's performance can be published and communicated.
- Normally, there will be at least an annual review of performance and then a revision of processes, and the setting of revised performance objectives for the following period.
- This risk management performance assessment is an integral part of the overall organization's performance assessment and measurement system for departments and individuals.

Checking any Risk Management System

- The Certification in Risk Management Assurance® (CRMA®) focuses on the key elements to unlocking internal audit's full potential, and validates one's ability to provide advice and assurance on risk management to audit committees and executive management.

Earning the CRMA helps address the impact of risk and demonstrates you have the ability to:

- Provide assurance on core business processes in risk management and governance.
- Educate management and the audit committee on risk and risk management concepts.
- Offer quality assurance and control self-assessment.
- Focus on strategic organizational risks.



https://na.theiia.org/certification/crma-certification/pages/crma-certification.aspx

Risk Management for „Adults“

- What am I trying to achieve?
- What is affecting my objectives?
- Which causes and effects exist?
- Which are the big ones?
- What can I do about it?
- What are the costs of the implementation vs the benefit of the risk reduction?
- What has changed?
- Who is the target group of my risk report?

Risk and oppurtunities…

…are both sides of the coin…

DR.FISCHER
MANAGEMENTBERATUNG

: Bachgasse 4,
A – 3002 Purkersdorf
: +43-2231-61813
: +43-2231-61813
: +43 699 102 408 25
: franz.fischer@fischer-consult.at
: https://fischer-consult.at/

Copyright & Picture credits

Slide: ©Lihua Peng

Content:

- M.o.R. Management of Risk (UK Gvt)
- RAMP Risk Analysis and Management for Projects (CE)
- PRINCE2 PRojects IN Controlled Environments (UK)
- PMI Project Management Institute (US)
- IPMA Int. Project Mgmt Association ICB4 (EU, Pac Asia)
- COBIT 5 Enterprise Risk Management
- COSO Framework for Risk Management
- ONR 49000 Austrian-Suisse Alternative
- ISO 31000 Standard for Risk Management
- IIA – CRMA Standards