ISACA®
Trust in, and value from, information systems

COBIT® 5

AN ISACA® FRAMEWORK

COBIT 5 for Risk – An overview

Introduction

Steven Babb

sababb@email.com

- **Education**
  - 1st Class BSc (Hons) Computing
  - BS7799 Lead Auditor, ITIL Service Manager
  - Prince 2 Certified Practitioner, CGEIT, CRISC
- **Professional Career**
  - International Brewer, various roles (1991-1996)
  - KPMG, Service Line Leader, IT risk management (1996-2012)
  - Betfair, Head of Governance, Risk & Assurance (2012-…)
- **ISACA involvement – past and present**
  - *RiskIT* TF, COBIT 5 TF, Cloud Computing TF
  - Knowledge Board member, Framework Committee Chair
  - COBIT 5 for Risk TF Chair, COBIT Growth Strategy TF

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

Objectives

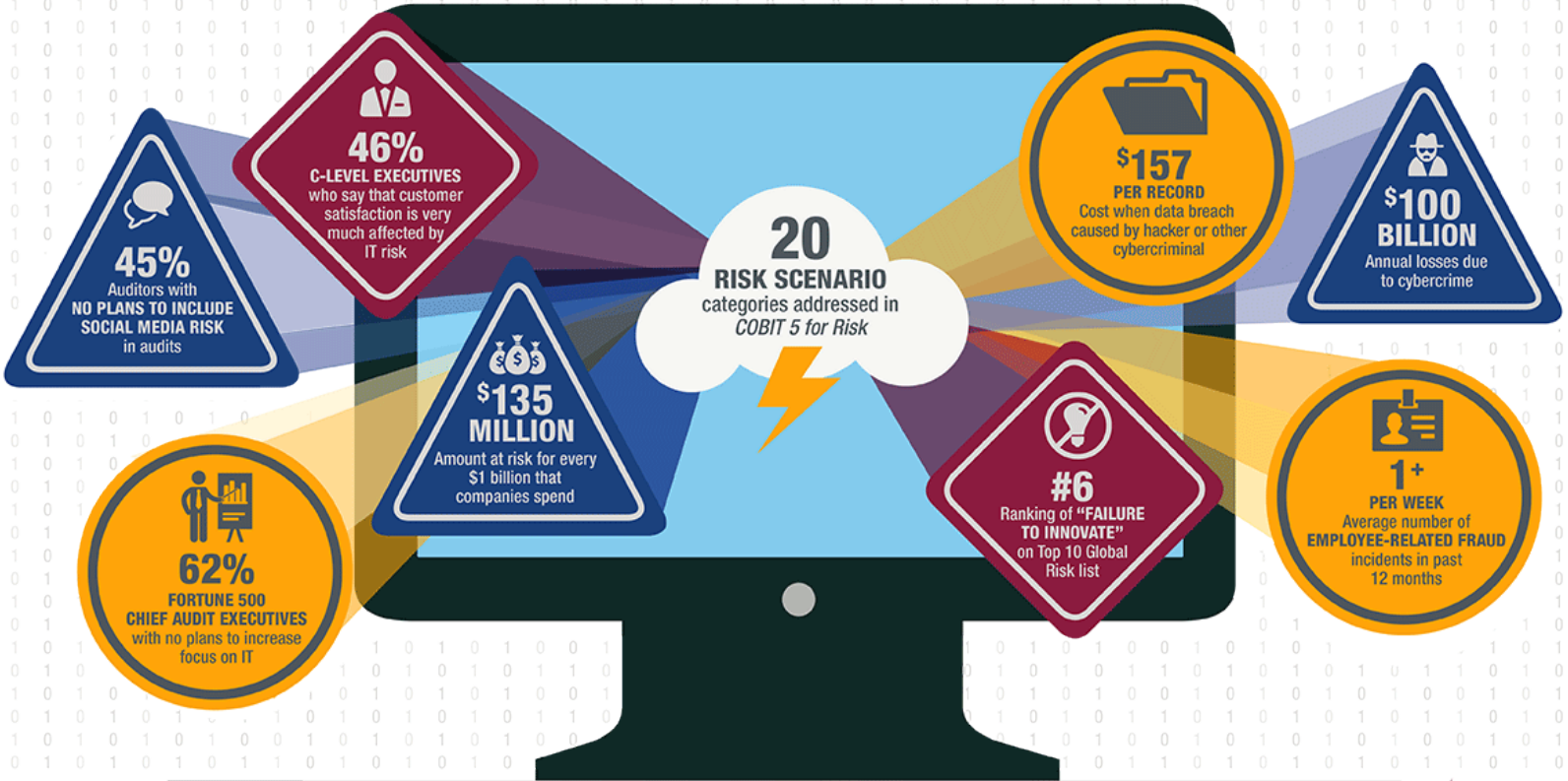
- **After completing this session, you will:**
  - Be clear on the **drivers**, **benefits** and **target audience** for COBIT 5 for Risk
  - Understand the **two perspectives** on how COBIT 5 for Risk can be used
  - Understand how to use **risk scenarios** and COBIT 5 enablers for governing and managing risk activities
  - Understand how COBIT 5 for Risk **relates and aligns** to other standards

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

THE IT RISK EFFECT

Failing to include technology risk in enterprise risk can have major impact



COBIT 5 AN ISACA® FRAMEWORK

SOURCES:

The Economic Impact of Cyber Crime and Cyber Espionage, Center for Strategic and International Studies, July 2013. *2013 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, May 2013. *2012 IBM Global Reputational Risk and IT Study. The Risk of Insider Fraud*, Ponemon Institute, February 2013. *Pulse of the Profession*, IIA, 2013. *2013 Internal Audit Capabilities and Needs Survey Report*, Protiviti. *Global Risk Management Survey 2013*, Aon Risk Solutions. *2013 Pulse of the Profession*, Project Management Institute, March 2013. *COBIT 5 for Risk*, ISACA, 2013.

ISACA® Trust in, and value from, information systems

COBIT® 5
AN ISACA® FRAMEWORK

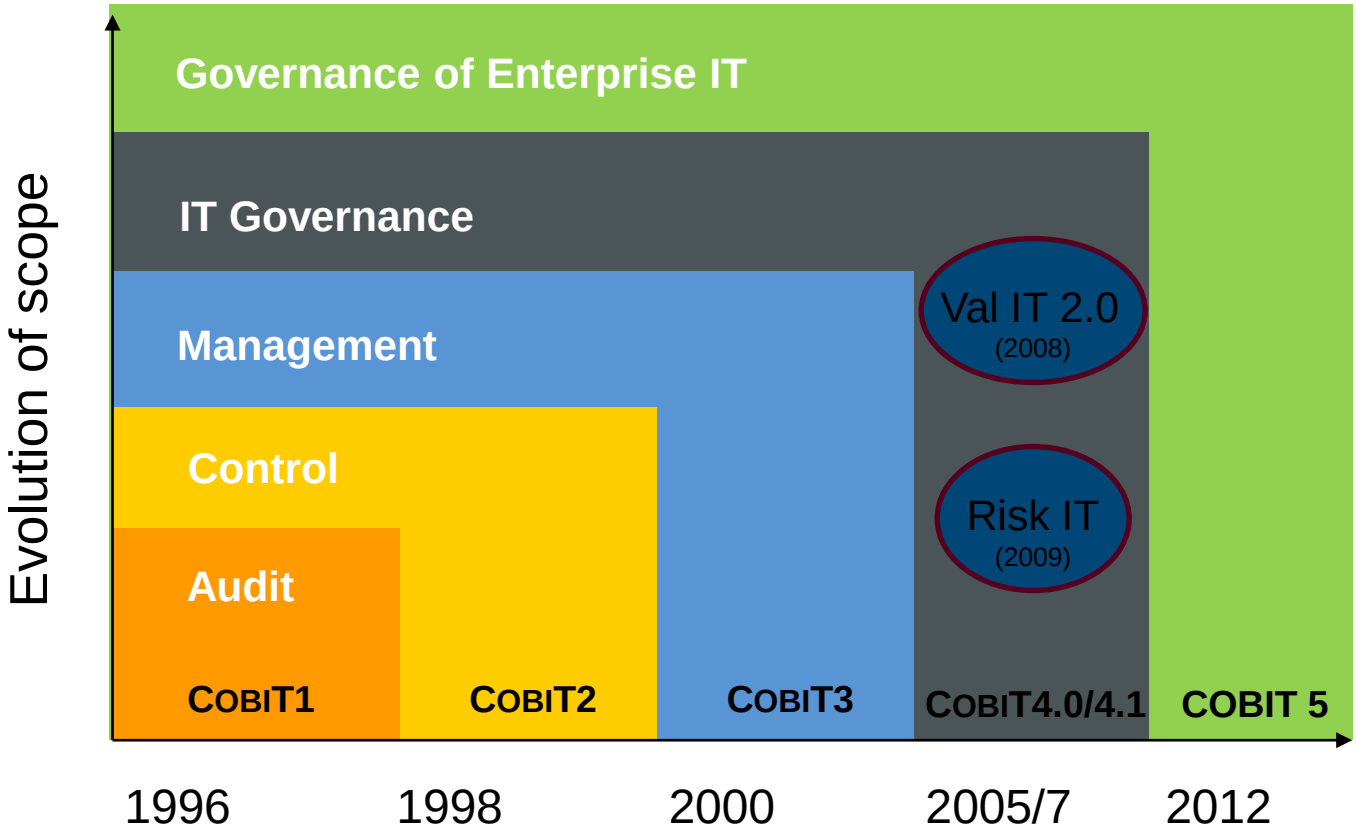
ISACA®
Trust in, and value from, information systems

The COBIT 5 journey… so far

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

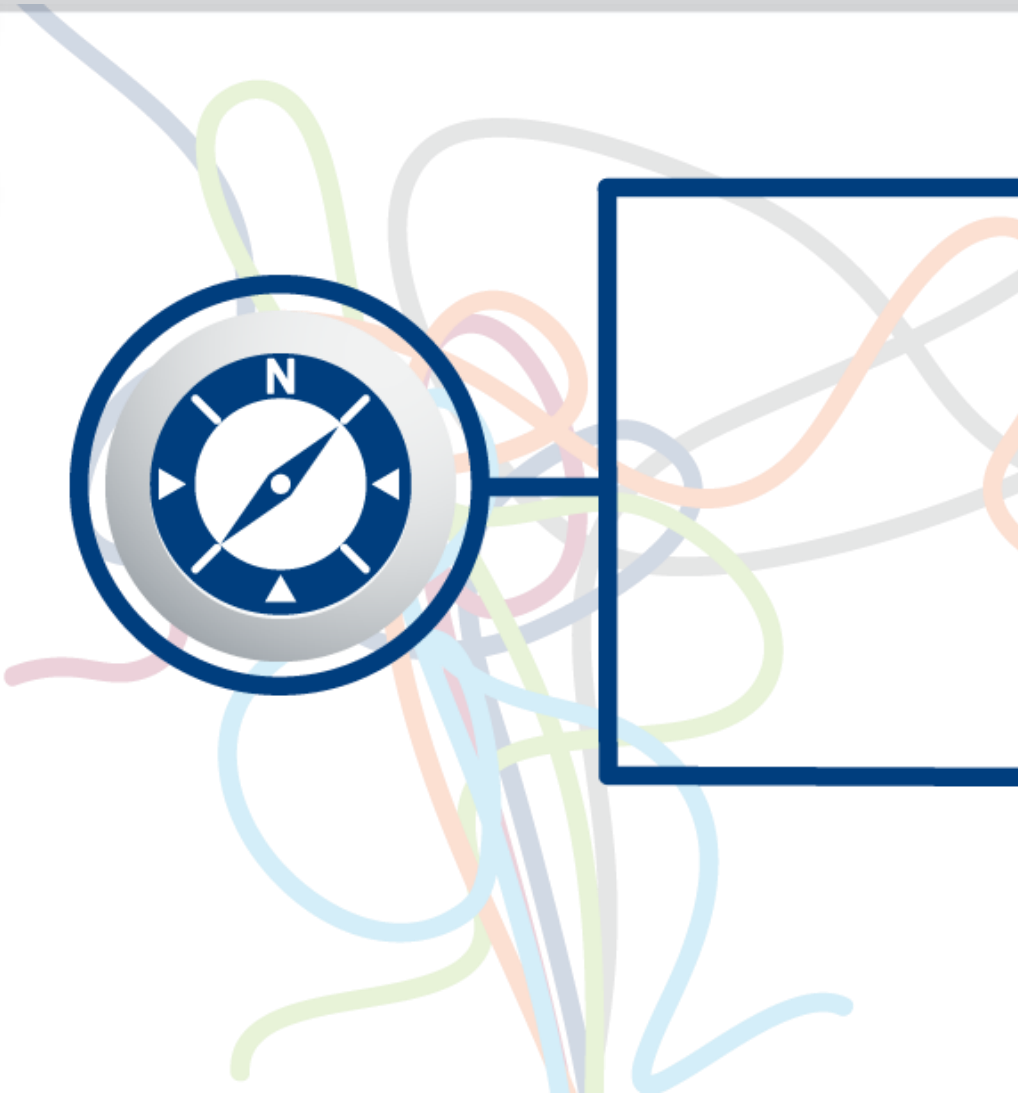
Development history



COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

April 2012



Release of COBIT 5

- COBIT 5 Framework
- COBIT 5 Implementation Guide
- COBIT 5: Enabling Processes

IT professionals and CIOs need up-to-date tools and expertise to navigate an increasingly complex business environment

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

June 2012

Release of COBIT 5 for Information Security

Leverages the COBIT 5 framework through a security lens

Provides guidance to help IT and security professionals understand, utilise, implement and direct important information security-related activities

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

January 2013

Release of the COBIT 5 Assessment Programme

- COBIT Process Assessment Model: Using COBIT 5
- COBIT Assessor Guide: Using COBIT 5
- COBIT Self-Assessment Guide: Using COBIT 5

Provides a clear process assessment capability and helps enterprises ensure strong, reliable and consistent processes

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

May 2013

Release of COBIT 5 for Assurance

Leverages the COBIT 5 framework through an assurance lens

Provides guidance for Assurance professionals and other interested parties at all levels on how to use COBIT 5 to support a variety of IT assurance activities.

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

September 2013

Release of COBIT 5 for Risk

Leverages the COBIT 5 framework through a risk management lens

Provides guidance to help risk professionals manage risk and incorporate IT risk into enterprise risk management, and to help IT and business management understand how to identify and manage IT risk effectively

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

November 2013

Release of COBIT 5 for Enabling Information

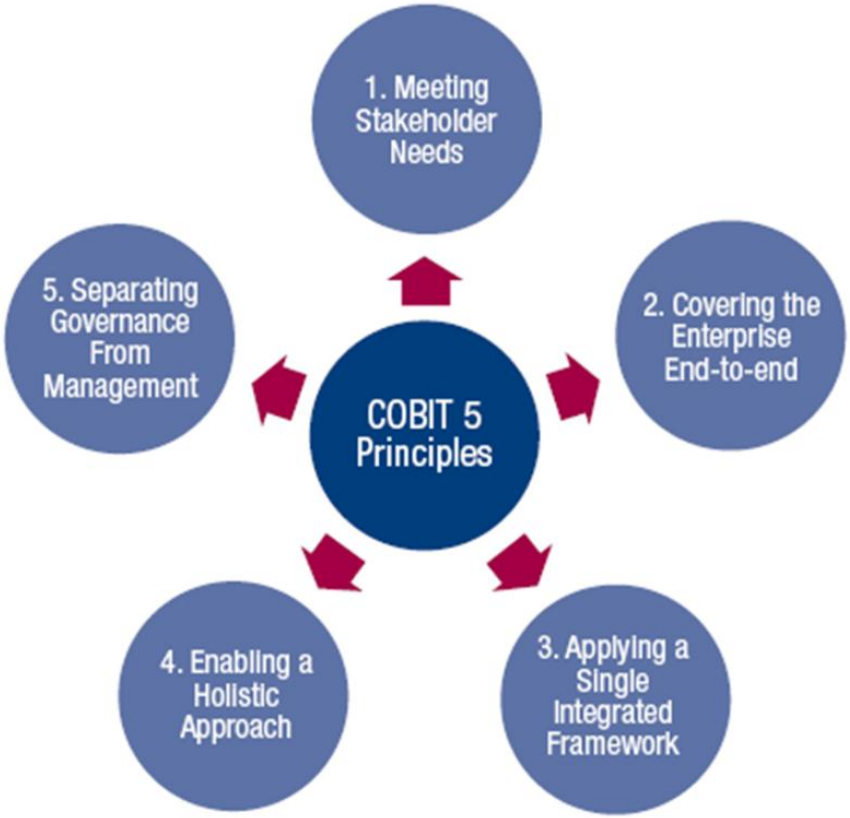
Leverages the COBIT 5 framework through an information management lens

A reference guide that provides a structured way of thinking about information governance and management issues. This can be applied throughout the life cycle of information, from conception and design, through building information systems, securing information, using and providing assurance over information, and to the disposal of information

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

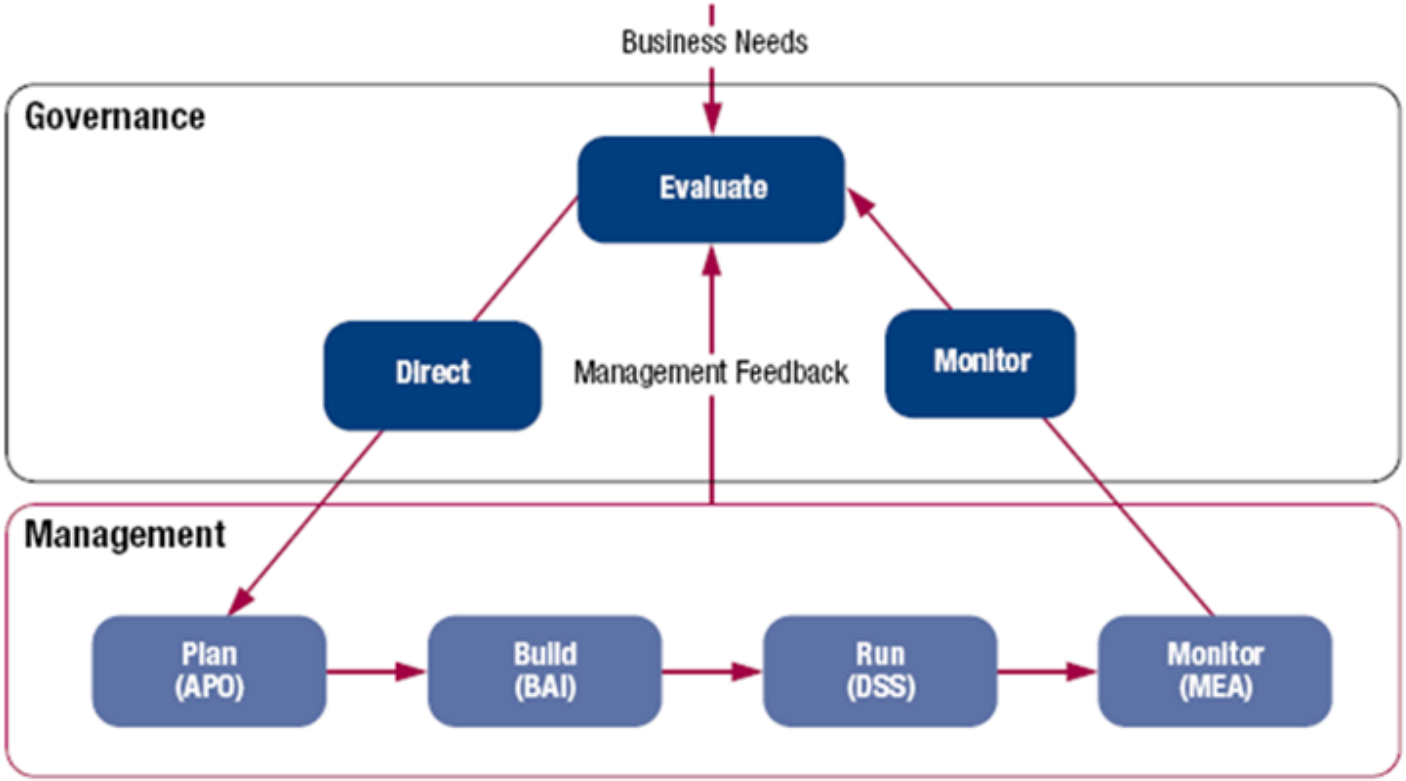
The COBIT 5 principles



COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

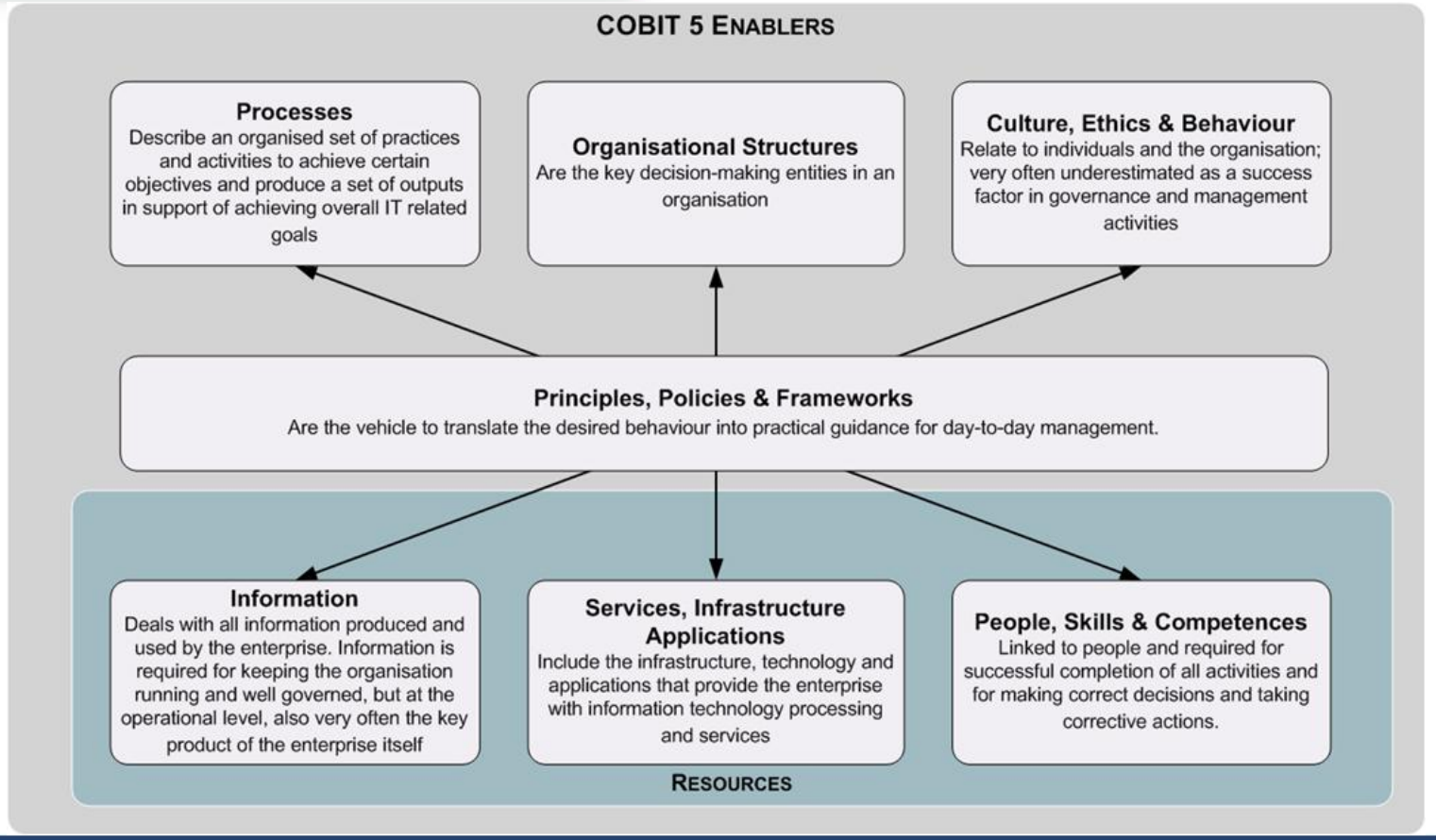
Governance and Management



COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

The COBIT 5 enablers

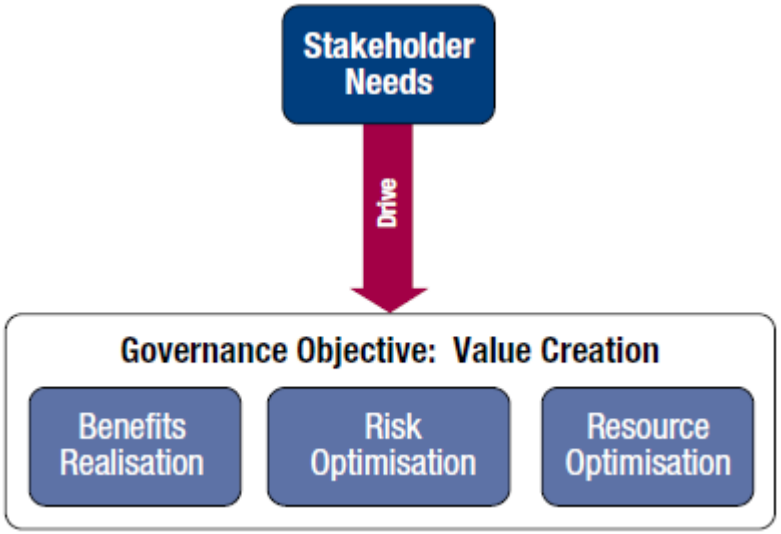


COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Stakeholder needs

- Enterprises exist to **create stakeholder value**
- Any enterprise, commercial or not, has **value creation as a governance objective**
- Value creation means **realising benefits** at an **optimal resource** cost while **optimising risk**
- Benefit forms, e.g., **financial** for commercial enterprises or **public service** for public bodies
- Risk optimisation is therefore an **essential part** of any governance system
- Risk optimisation cannot be seen in isolation, i.e., actions taken as part of **risk management will influence** benefits realisation and resource optimisation.



COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

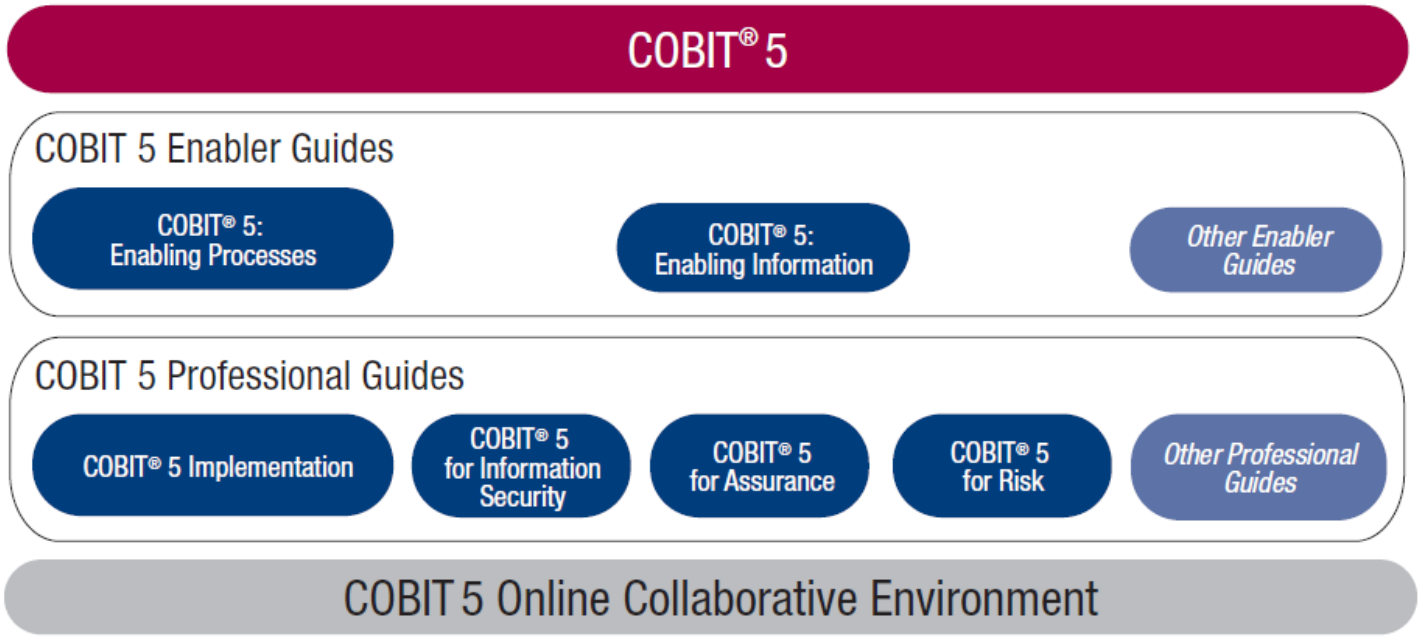
Value creation

- Governance objectives need to be translated into **manageable goals**
- This is the **COBIT 5 goals cascade**
- This translates stakeholder needs into **specific**, **actionable** and **customised** goals

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

Product Portfolio



COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

What's new?

- Developed in response to demand for specific risk guidance based on COBIT 5
- ISACA also saw a general need globally for better IT-related risk management and governance
- Builds on the success of *RiskIT*, ISACA's initial first IT risk management framework:
  - The risk scenarios have been updated and extended
  - COBIT 5 for Risk has no separate process model – everything is integrated into the COBIT 5 processes
  - COBIT 5 for Risk describes how to use the COBIT 5 enablers (the enabler model is a key difference in COBIT 5) to build and sustain an internal risk function

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

COBIT 5 for Risk – Example use cases

- **Use Case 1** – I have an established risk management function and want to understand its effectiveness
- **Use Case 2** – I am establishing a new risk management function and want to ensure it is setup effectively
- **Use Case 3** – I want to ensure my existing risk management processes are effective and are adding value back to the business
- **Use Case 4** – I want to understand what risk scenarios I should be considering for my risk assessments

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

What are the drivers, benefits and target audience for COBIT 5 for Risk

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Drivers for risk management

The main drivers for risk management include providing:

- Stakeholders with **substantiated and consistent opinions** over the current state of risk throughout the enterprise
- Guidance on how to **manage risk** to levels within the enterprise's **risk appetite**
- Guidance on how to set-up the right **risk culture** for the enterprise
- Wherever possible, **quantitative risk assessments** enabling stakeholders to consider the **cost of mitigation** and the required resources against the **loss exposure**

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

Drivers for COBIT 5 for Risk

To meet these drivers, COBIT 5 for Risk provides:

- Guidance on how to use the COBIT 5 Framework to establish the **risk governance and management function(s)** for the enterprise
- Guidance and a structured approach on how to use the COBIT 5 Principles to **govern and manage IT Risk**
- A **clear understanding** on the alignment of COBIT 5 for Risk with other relevant standards

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

Benefits

Which in turn brings a number of *benefits*:

- **End-to-end guidance** on how to manage risk
- A **common and sustainable approach** for assessment and response
- A **more accurate view** of significant current and near-future risk throughout the Enterprise – and the impact of this risk on the Enterprise
- Understanding how effective IT risk management **optimises value** by enabling process effectiveness and efficiency
- **Opportunities for integration** of IT risk management with the overall risk and compliance structures within the enterprise
- **Promotion of risk responsibility** and its acceptance throughout the enterprise

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

Target audience

The intended audience for COBIT 5 for Risk is extensive – the target audience includes:

- Risk professionals across the enterprise
  - assistance with managing IT risk and incorporating IT risk into ERM
- Boards and executive management
  - understanding of their responsibilities and roles with regard to IT risk management
  - the implications of risk in IT to Enterprise strategic objectives
  - how to better optimise IT use for successful strategy execution
- IT and business management
  - understanding of how to identify and manage IT risk and how to communicate IT risk to business decision makers

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Key questions

- **What is IT risk?**

  IT risk is defined as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise

- **How are the COBIT 5 enablers used to provide risk management?**

  They are used to provide two perspectives on how to use COBIT 5:
  - *The risk function perspective – what is needed in an enterprise to establish a risk function*
  - *The risk management perspective – how the core risk management process of identifying, analysing and responding to risk are delivered*

- **How do I set up and maintain an efficient risk function?**

  COBIT 5 for Risk provides guidance on what is needed to set up and maintain an effective and efficient risk function. It does so by listing and briefly describing the COBIT 5 enablers required, e.g., processes, organisational structures, culture, ethics and behaviour

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

Key questions

- **Are there any practical examples of risk scenarios provided?**

  Yes. A comprehensive list of example IT-related risk scenarios are provided, as well as some practical advice on how to best use these example scenarios

- **How does COBIT 5 for Risk help me in responding to risk?**

  COBIT 5 for Risk makes the link between risk scenarios and an appropriate response. Examples are also given on how risk scenarios can be mitigated through COBIT 5 enablers (controls)

- **Does COBIT 5 align with risk management standards?**

  Yes. A detailed comparison, in the form of a mapping or qualitative description, is included for a number of related standards

- **Does COBIT 5 for Risk help me in defining detailed risk analysis methods?**

  No. Additional guidance on detailed risk analysis methods, taxonomies, tools, etc., is available from multiple sources, including ISACA

COBIT® 5
AN ISACA® FRAMEWORK

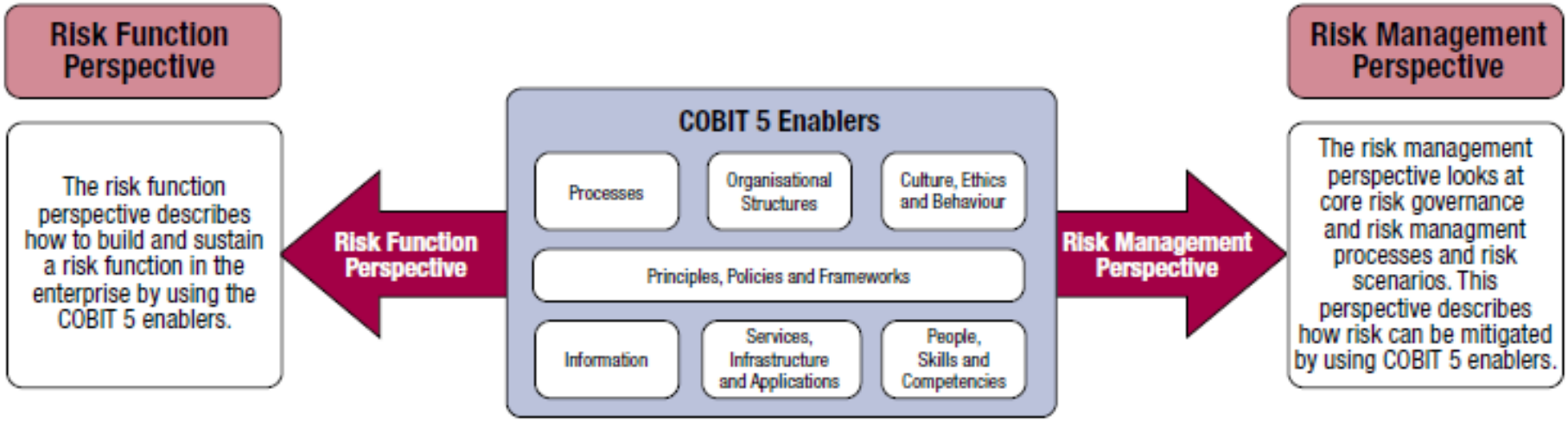
ISACA®
Trust in, and value from, information systems

What are the two perspectives on how COBIT 5 for Risk can be used

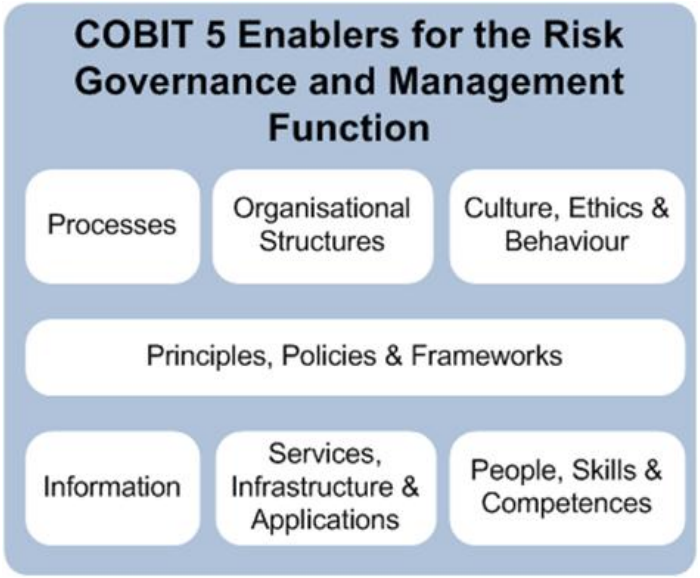
COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Risk perspectives



Risk Function Perspective



COBIT 5 for Risk provides guidance and describe how each enabler contributes to the overall governance and management of the risk function. For example, which:

- **Processes** are required to define and sustain the risk function, govern and manage risk
- What **Information flows** are required to govern and manage risk – e.g. risk universe, risk profile, etc.
- The **Organisational structures** that are required to govern and manage risk effectively – e.g. Enterprise risk committee, risk function, etc.
- What **People and Skills** should be put in place to establish and operate an effective risk function

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Risk Function Perspective

COBIT 5 for Risk defines 7 risk principles, in order to:

- Provide a **systematic**, **timely** and **structured approach** to risk management
- Contribute to **consistent**, **comparable** and **reliable** results

The risk principles **formalise** and **standardise** policy implementation – both the core IT risk policy and supporting policies – e.g. information security policy, business continuity policy

These policies provide more detailed guidance on how to put **principles into practice** and how they will **influence decision making** within an enterprise

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

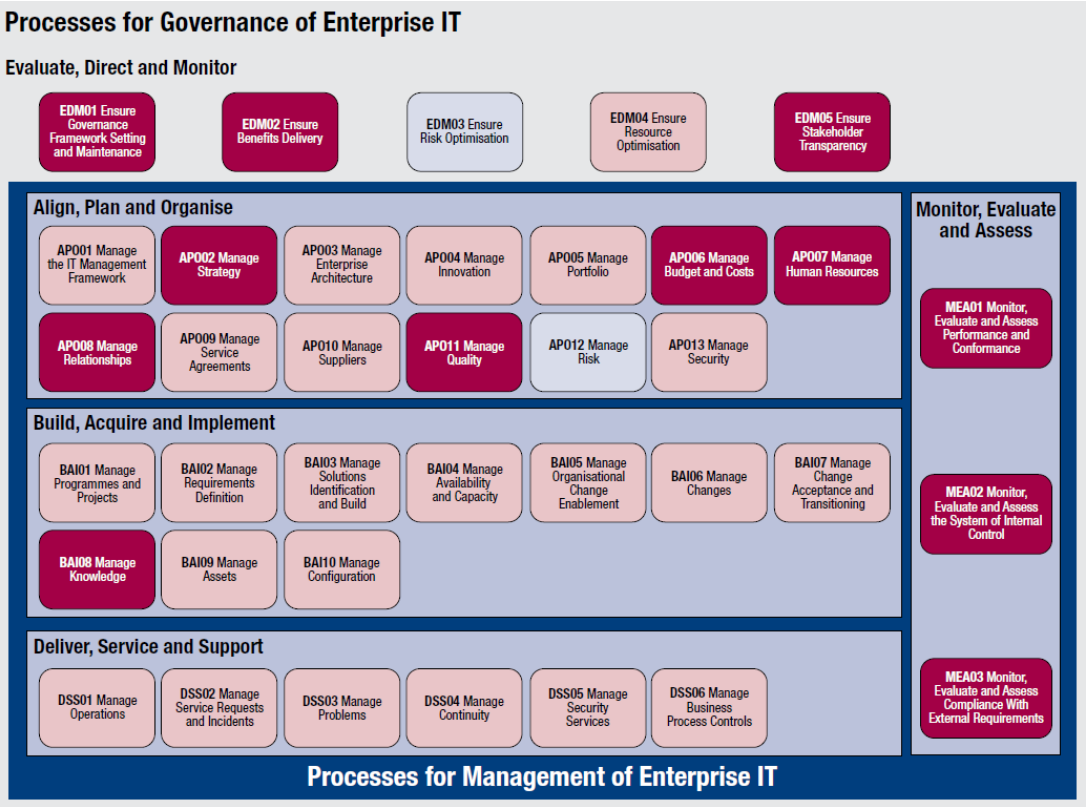
Risk Function Perspective

COBIT 5 for Risk identifies all COBIT 5 processes that are required to support the risk function:

- ***Key*** *supporting processes* – dark pink
- ***Other*** *supporting processes* – light pink

Core risk processes, shown in light blue are also highlighted – these processes support the **Risk Management Perspective**:

- EDM03 – Ensure risk optimisation
- APO12 – Manage risk



COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

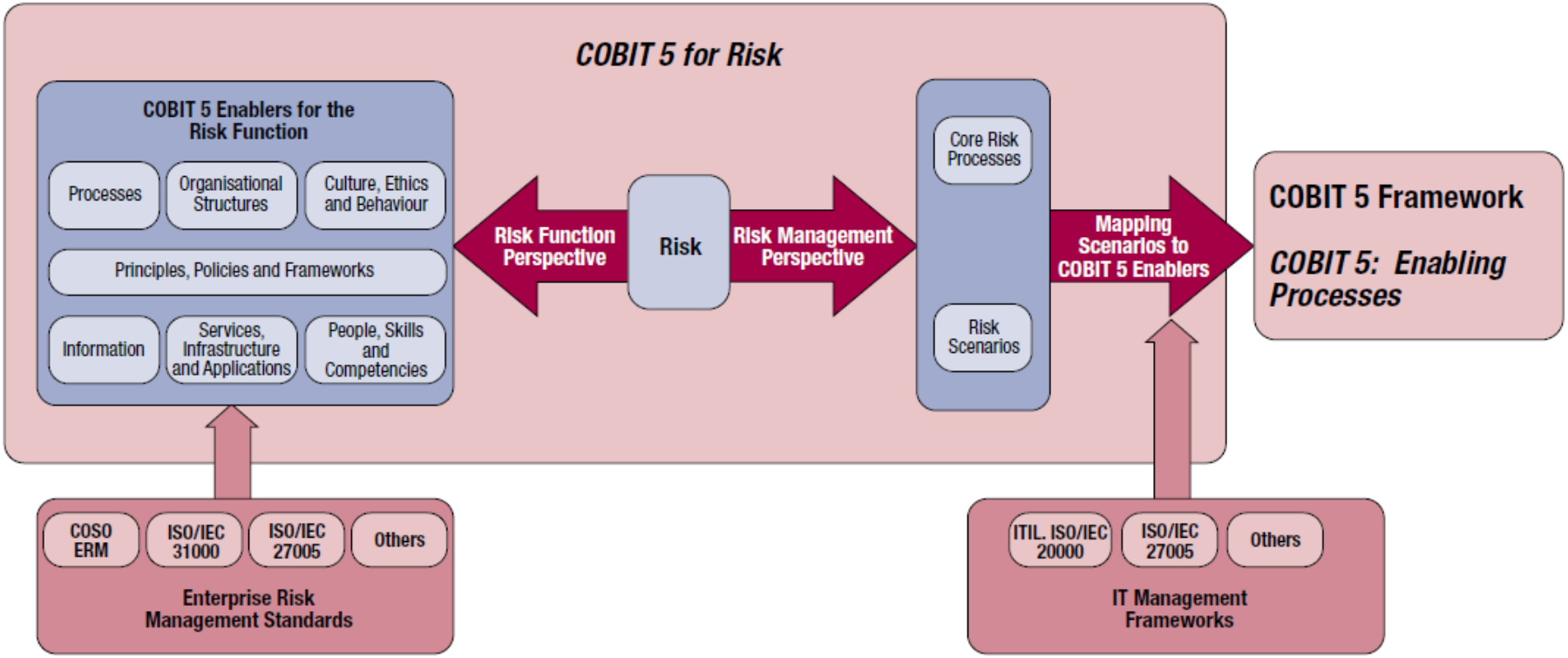
Risk Management Perspective

COBIT 5 Process Identification	Reasoning
EDM03 Ensure Risk Optimisation	This process covers the understanding, articulation and communication of the enterprise risk appetite and tolerance and ensures identification and management of risk to the enterprise value that is related to IT use and its impact. The goals of this process are to: • Define and communicate risk thresholds and make sure that key IT-related risk is known. • Effectively and efficiently manage critical IT-related enterprise risk. • Ensure IT-related enterprise risk does not exceed risk appetite.
APO12 Manage Risk	This process covers the continuous identification, assessment and reduction of IT-related risk within levels of tolerance set by enterprise executive management. Management of IT-related enterprise risk should be integrated with overall ERM. The costs and benefits of managing IT-related enterprise risk should be balanced by: • Collecting appropriate data and analysing risk • Maintaining the risk profile of the enterprise and articulating risk • Defining the risk management action portfolio and responding to risk

COBIT 5 for Risk provides specific guidance related to all enablers for the effective management of risk:

- The core **Risk Management process(es)** used to implement effective and efficient risk management for the enterprise in order to support stakeholder value
- **Risk Scenarios**, i.e. the key information item needed to identify, analyse and respond to risk; Risk scenarios are the concrete, tangible and assessable representation of risk
- How **COBIT 5 enablers** can be used to **respond** to unacceptable risk scenarios

Risk perspectives



COBIT® 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

How should I use risk scenarios and COBIT 5 enablers for governing and managing risk activities

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

Risk scenarios

Definition

"A risk scenario is a description of a **possible event** that, when occurring, will have an **uncertain impact** on the achievement of the enterprise's objectives. The impact can be **positive** or **negative**"

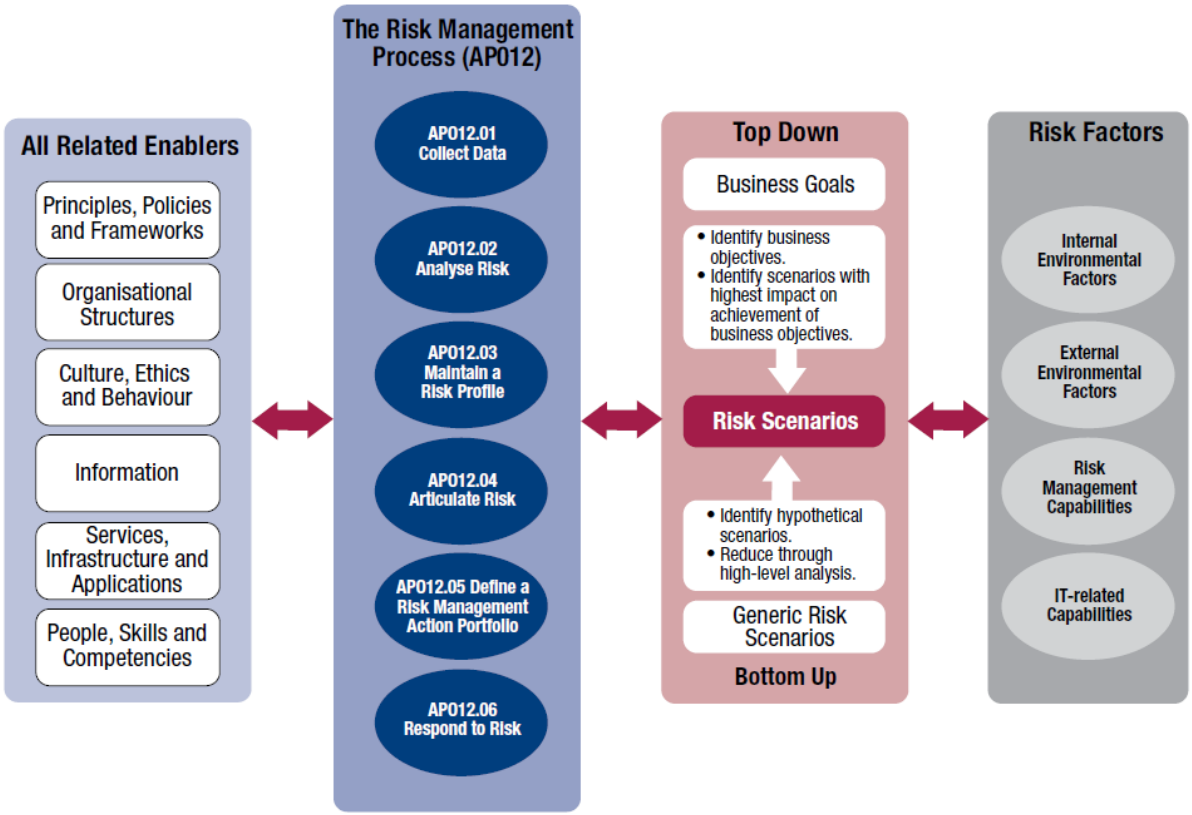
COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Risk scenarios

Risk scenario's are a key element of the COBIT 5 risk management process APO12; two approaches are defined:

- **Top-down approach** – Use the overall enterprise objectives and consider the most relevant and probable IT risk scenarios impacting these
- **Bottom-up approach** – Use a list of generic scenarios to define a set of more relevant and customised scenarios, applied to the individual enterprise



COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Risk scenarios

- **Top-down** and **Bottom-up** – Both approaches are complementary and should be used simultaneously
- Risk scenarios must be **relevant and linked** to real business risk
- Specific risk items for each enterprise and critical business requirements need to be considered in the enterprise risk scenarios
- COBIT 5 for Risk provides a comprehensive set of generic risk scenarios – **these should be used as a reference** to reduce the chance of overlooking major/common risk scenarios

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Risk scenarios

COBIT 5 for Risk provides:

- **111 risk scenario** examples
- across **20 scenario categories**

Ref.	Risk Scenario Category	Risk Type			Example Scenarios	
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Positive Example Scenarios
1001	Business ownership of IT	P	P	S	Business does not assume accountability over those IT areas it should, e.g., functional requirements, development priorities, assessing opportunities through new technologies.	Business assumes appropriate accountability over IT and co-determines the strategy of IT, especially application portfolio.
1002		P	S	S	There is extensive dependency and use of end-user computing and *ad hoc* solutions for important information needs, leading to security deficiencies, inaccurate data or increasing costs/inefficient use of resources.	
1003		P	S	S	Cost and ineffectiveness is related to IT related purchases outside of the procurement process.	A business case is always made up to ensure optimal cost and effective purchasing of software.
1004				P	Inadequate requirements lead to ineffective service level agreements (SLAs).	

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Risk response

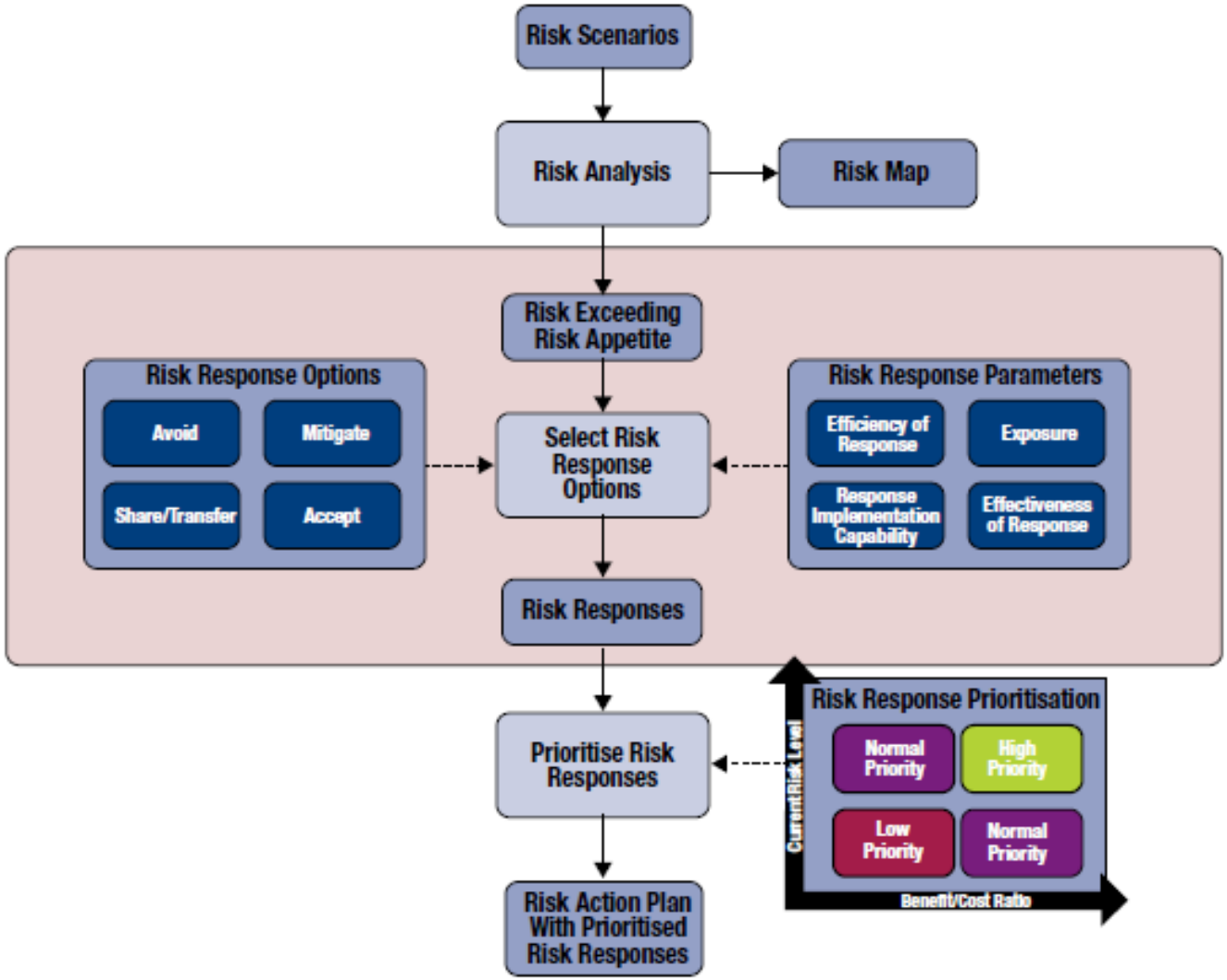
- To **bring risk in line** with the risk appetite for the enterprise
- A response needs to be defined such that as much future residual risk as possible (current risk with the risk response defined and implemented) falls within **accepted** limits
- When risk analysis has shown that risk is not aligned with the defined risk appetite and tolerance levels, a response is required
- This response can be any of the four possible responses:
  - **Avoid, Mitigate, Share/Transfer, Accept**
- **Risk response evaluation is not a one-time effort** – it is part of the risk management process cycle

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Risk mitigation

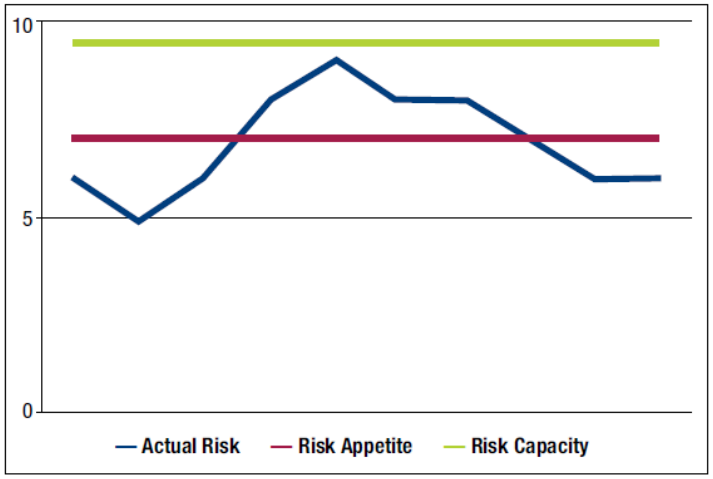
- COBIT 5 for Risk provides **a number of examples** on how the COBIT 5 enablers can be used to respond to risk scenarios
- Risk mitigation is **equivalent to implementing** a number of IT controls
- In COBIT 5 terms, **IT controls can be any enabler**, e.g.,
  - putting in place an organisational structure, putting in place certain governance or management practices or activities, etc.
- For each of the 20 risk scenario categories, potential mitigating actions relating to all seven COBIT 5 enablers are provided, with a reference, title and description for each enabler that can help to mitigate the risk

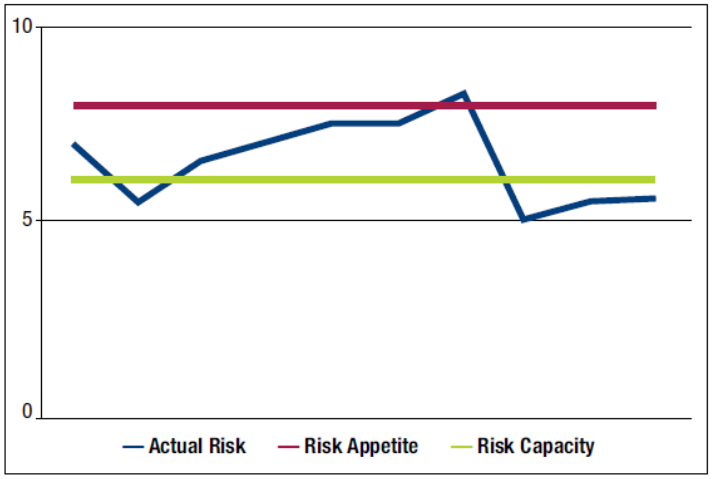

Risk Scenarios
Risk Analysis
Risk Map
Risk Exceeding Risk Appetite
Risk Response Options
Avoid
Mitigate
Share/Transfer
Accept
Select Risk Response Options
Risk Response Parameters
Efficiency of Response
Exposure
Response Implementation Capability
Effectiveness of Response
Risk Responses
Prioritise Risk Responses
Risk Response Prioritisation
Normal Priority
High Priority
Low Priority
Normal Priority
Current Risk Level
Benefit/Cost Ratio
Risk Action Plan With Prioritised Risk Responses

Risk Capacity

- ***Risk Appetite*** – The broad-based **amount of risk** in different aspects that an enterprise is willing to accept in pursuit of its mission
- ***Risk Tolerance*** – The **acceptable level of variation** that management is willing to allow for any particular risk as it pursues objectives
- ***Risk Capacity*** – The **cumulative loss** an enterprise **can tolerate** without risking its continued existence. As such, it differs from risk appetite, which is more on how much risk is desirable

Risk Capacity





- Left diagram – A relatively **sustainable** situation
  - Risk appetite is lower than risk capacity
  - Actual risk exceeds risk appetite in a number of situations, but always remains below the risk capacity
- Right diagram – An **unsustainable** situation
  - Risk appetite is defined at a level beyond risk capacity; this means that management is prepared to accept risk well over its capacity to absorb loss
  - As a result, actual risk routinely exceeds risk capacity even when staying almost always below the risk appetite level. This usually represents an unsustainable situations

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

How COBIT 5 for Risk relates and aligns to other standards

Alignment

- COBIT 5 for Risk – much like COBIT 5 itself – **is an umbrella approach** for the provisioning of risk management activities
- COBIT 5 for Risk is **positioned in context** with the following risk-related standards:
  - ISO 31000:2009 – Risk Management
    - **addresses all** ISO 31000 principles
  - ISO 27005:2011 – Information security risk management
    - **addresses all** of the components described within ISO 27005
    - COBIT 5 for Risk takes a broader view – not just information security risk management
  - COSO Enterprise Risk Management
    - **addresses all** of the components defined in COSO ERM
    - COBIT 5 for Risk focuses less on control, but does link to COBIT 5 enablers

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

Objectives… met?

- **After completing this session, you will:**
  - Be clear on the **drivers**, **benefits** and **target audience** for COBIT 5 for Risk
  - Understand the **two perspectives** on how COBIT 5 for Risk can be used
  - Understand how to use **risk scenarios** and COBIT 5 enablers for governing and managing risk activities
  - Understand how COBIT 5 for Risk **relates and aligns** to other standards

In finishing

- Thank you for your interest in COBIT 5 for Risk
- To learn more, visit:
  - www.isaca.org/COBIT5
  - www.isaca.org/COBIT5forrisk