
THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL CONFERENCE
VANCOUVER, BC, CANADA / JULY 5-8, 2015
VANCOUVER2015
COBIT 5 for Risk
CS 3-7: Monday, July 6 4:00-5:00
Presented by: Nelson Gibbs
CIA, CRMA, CISA, CISM, CGEIT, CRISC, CISSP
ngibbs@pacbell.net
Mountains of Change...Oceans of Opportunities

Disclaimer of Use and Association

Note: It is understood that the material in this presentation is intended for general information only and should not be used in relation to any specific application without independent examination and verification of its applicability and suitability by professionally qualified personnel. Those making use thereof or relying thereon assume all risk and liability arising from such use or reliance. Whilst I took reasonable care in creating the information in this presentation, this presentation and its contents may contain errors, faults and inaccuracies, and may not be complete or current. If so, I apologize.

Any copyrighted material to which this presentation refers remains the sole and complete property of the copyright holder, and its inclusion herein is for educational and other fair use purposes only. I claim no originality or ownership of any of these materials; all included commentary has its roots in pre-existing prior work(s). If you own the rights to any of the material and wish it removed please let me know, I'm happy to work with you (and thank you for developing whatever it is I thought was valuable enough to share with others).

The views I am about to express are my own and do not necessarily represent the views of my employer, The IIA, or any other association or entity with which I might be, or reasonably be assumed to be, affiliated with. This presentation is not sponsored, endorsed, supported, or otherwise condoned by any entity, person, organization, sect, creed, or interested party other than myself.

Warning: Attendance at this presentation could cause you to experience fatigue, sensory overload, dry mouth, nausea, or outrage, but hopefully not vomiting.

Welcome!

- 20+ years in IT
  - Network/SysAdmin
  - Director, Information Technology & Services
  - Senior Manager, Deloitte AERS
  - Information Security & Risk Management Advisors, LLC
    - Design & implementation of an Information Security Governance program in conjunction with a transition to COBIT 5
    - Leveraging COBIT 5 for Information Security for a healthcare provider
  - Union Bank - Director, Sr. Audit Manager IT Risk & Gov.
- Increased organizational value through alignment and efficiency
- Optimal reliability through consistency and predictability
- Continuous improvement and shared learning

Information!

- Information is a key resource for all enterprises.
- Information is created, used, retained, disclosed and destroyed.
- Technology plays a key role in these actions.
- Technology is becoming pervasive in all aspects of business and personal life.

What benefits do information and technology bring to enterprises?

Enterprise Benefits

Enterprises and their executives strive to:

- Maintain quality information to support business decisions.
- Generate business value from IT-enabled investments, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT.
- Achieve operational excellence through reliable and efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimise the cost of IT services and technology.

How can these benefits be realised to create enterprise stakeholder value?

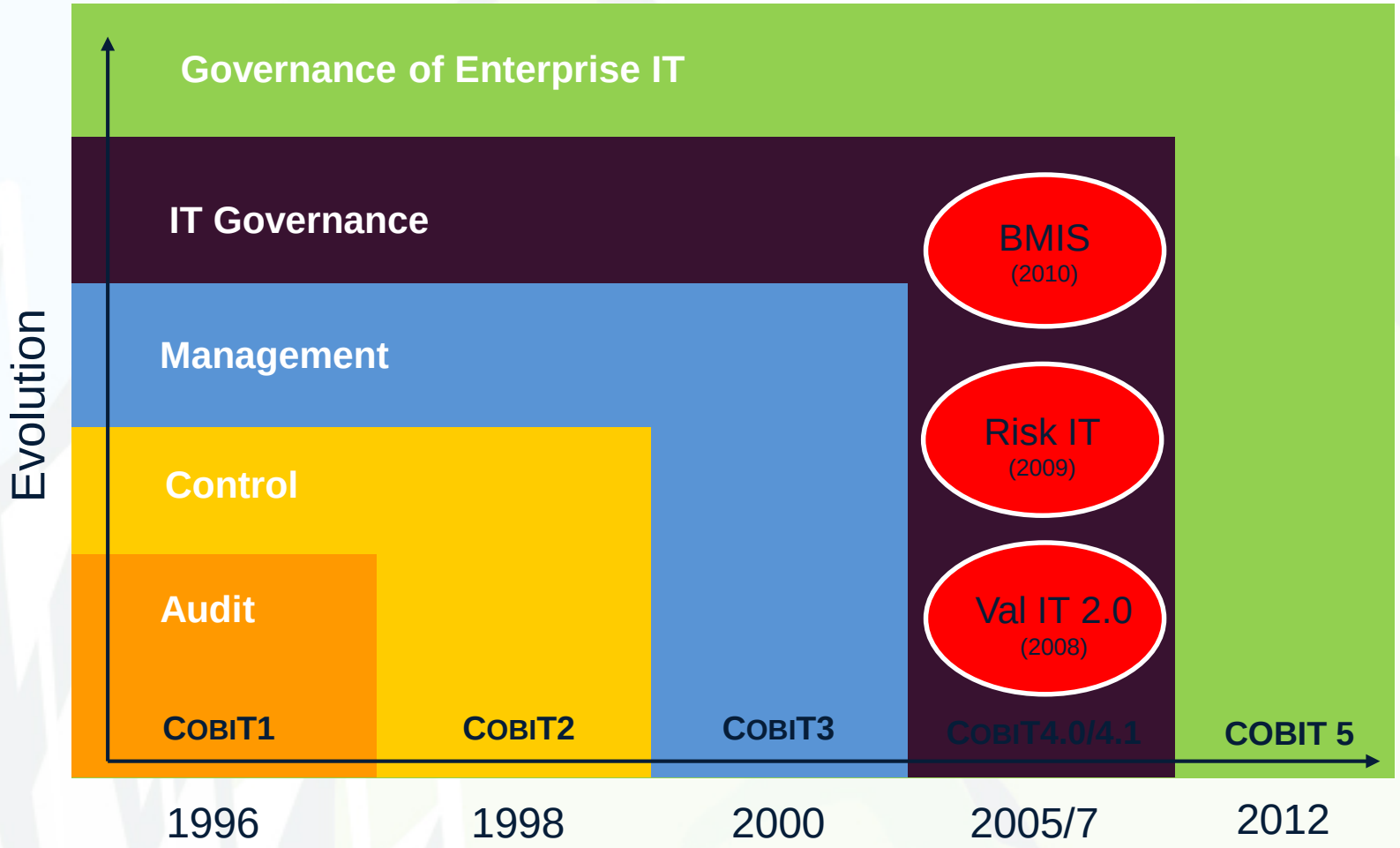
Stakeholder Value

- Delivering enterprise stakeholder value requires good **governance and management** of information and technology (IT) assets.
- Enterprise boards, executives and management have to **embrace IT** like any other significant part of the business.
- External **legal, regulatory and contractual compliance** requirements related to enterprise use of information and technology are increasing, threatening value if breached.
- **COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT**.

COBIT 5

MODEL & FRAMEWORK

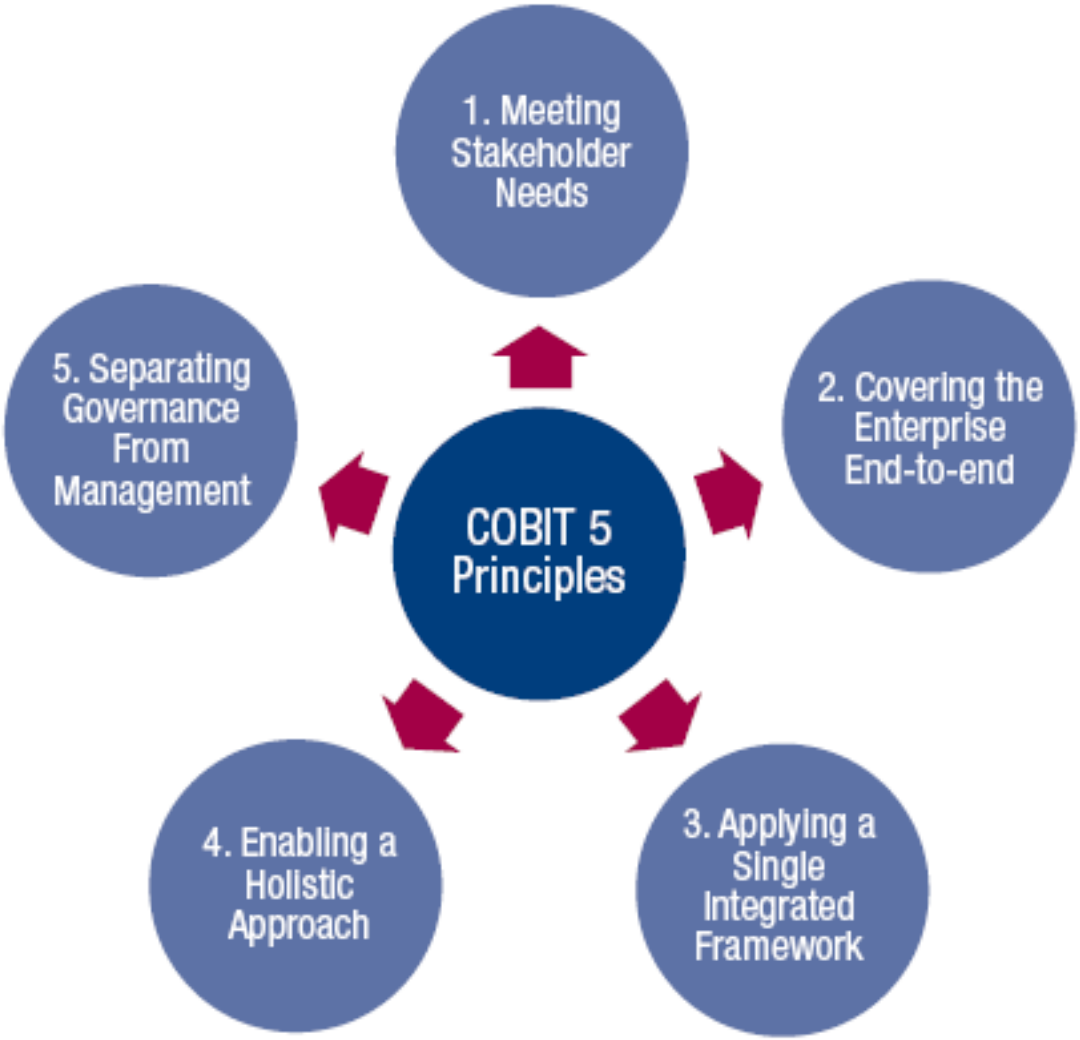
The Evolution of COBIT 5



The COBIT 5 Framework

- Simply stated, COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.
- COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.
- The COBIT 5 **principles** and **enablers** are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

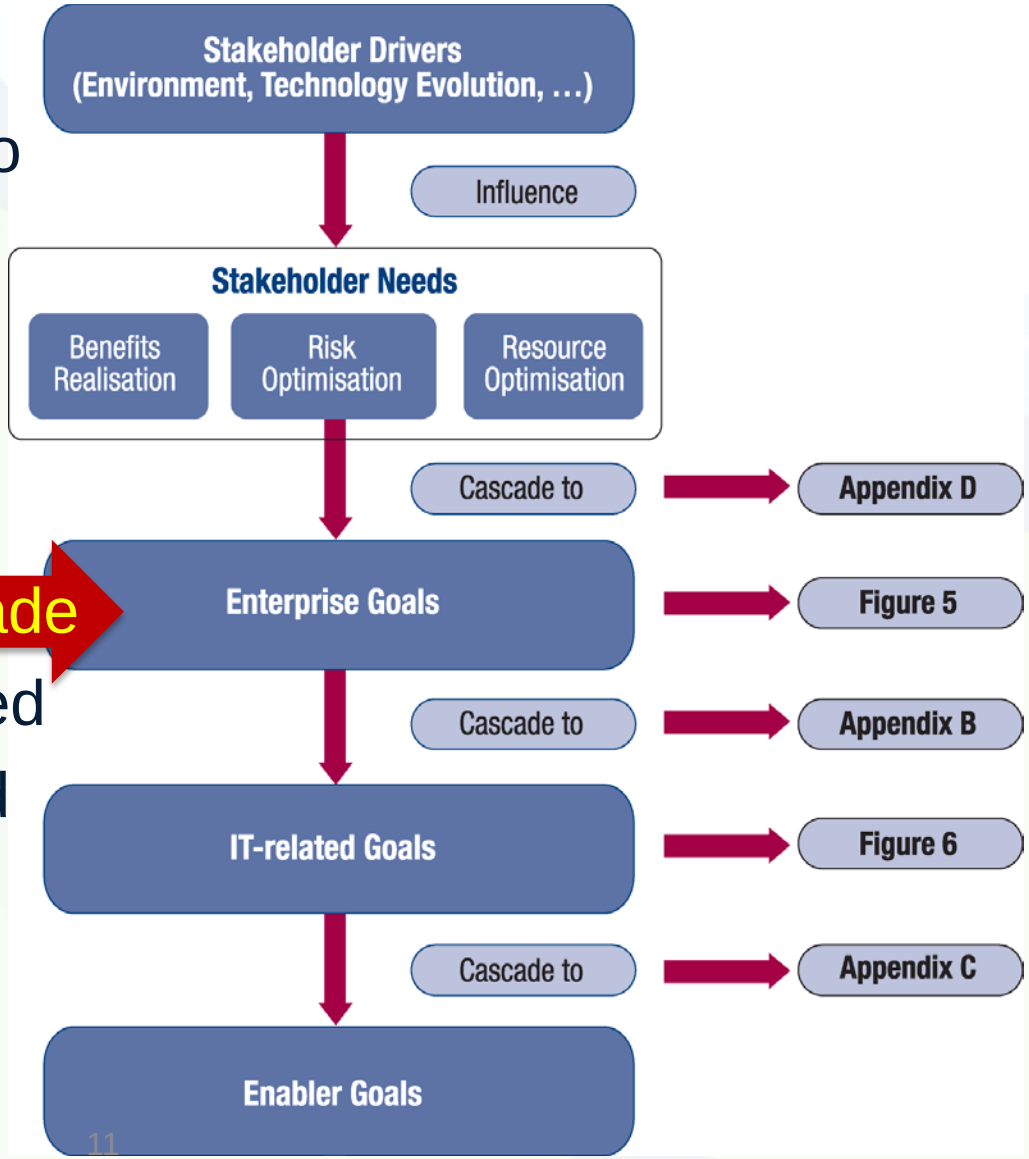
COBIT 5 Principles



Meeting Stakeholder Needs

Stakeholder needs have to be transformed into an Enterprise's actionable strategy

The COBIT 5 goals cascade translates stakeholder need into specific, practical and customized goals



Example

Stakeholder Driver – Marketplace Competition

Stakeholder Need – Retain and grow customer base

Enterprise Goal – "Value our Customers"

IT Goal – Protect the confidentiality of information

[Enabler Goals are defined in the COBIT framework – e.g. "Accessibility and Security"]

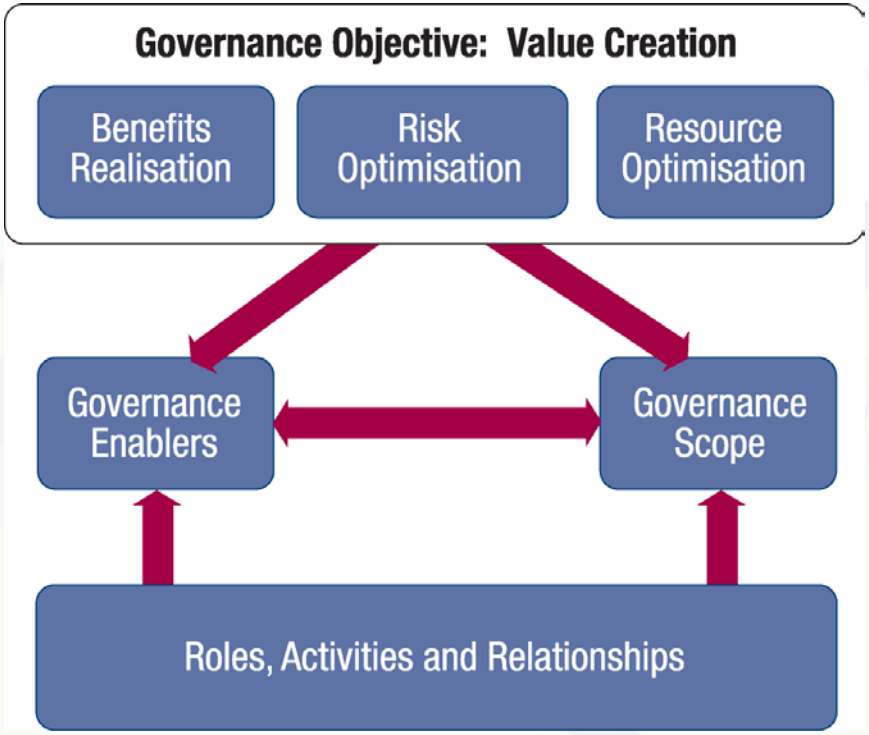
Process – DSS05: Manage Security Services

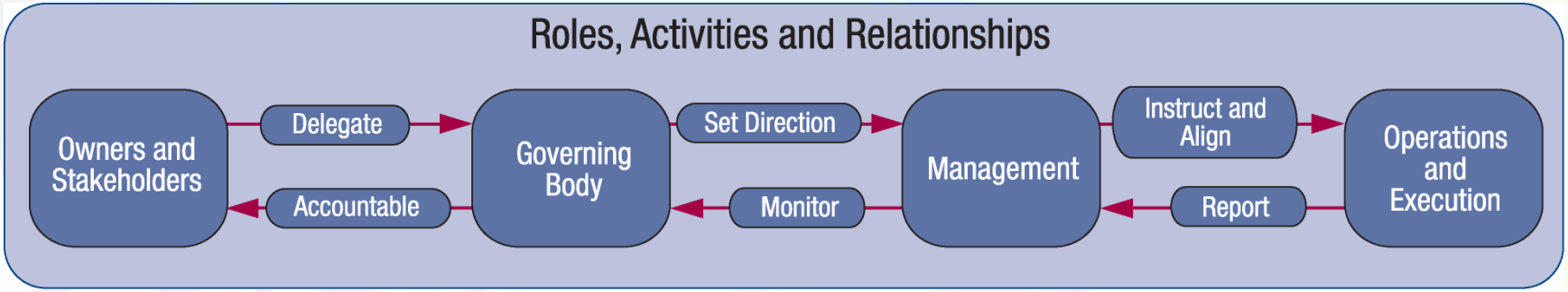
Management Practice – DSS05.01: Protect against malware

Activities:

- ***deploy and monitor current anti-virus tools using an automated, centralized solution (DSS05.01.2&3)***
- ***provide security awareness training to all employees (DSS05.01.6)***

Covering the Enterprise End-to-End





Applying a Single Integrated Framework

- The **COBIT 5** product family is the connection:
  - *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT– Released April 10 2012*
  - *COBIT 5: Enabling Processes – Released April 10 2012*
  - *COBIT 5 Implementation Guide – Released April 10 2012*
  - COBIT 5 for Information Security *– Released June 25, 2012*
  - COBIT 5 for Assurance *– Released May 29, 2013*
  - COBIT 5 for Risk *– Released October 2, 2013*
  - COBIT 5 Enabling Information *– Released November 13, 2013*
  - COBIT 5 Online *– Currently available with enhancements in development*
  - A series of other products is planned for specific audiences or topics
- The perspective concept links the above to external sources for standards

COBIT 5 Product Family

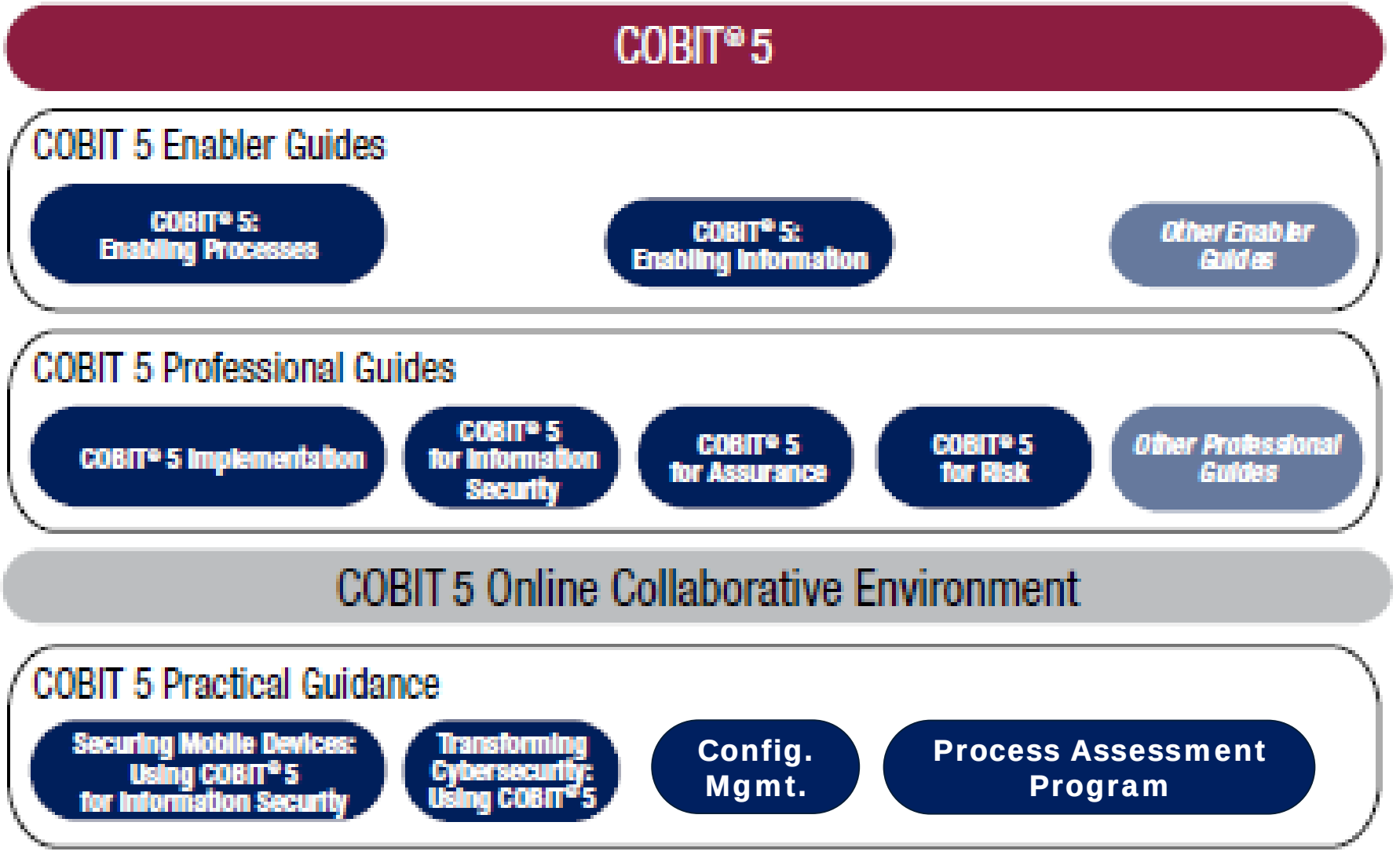
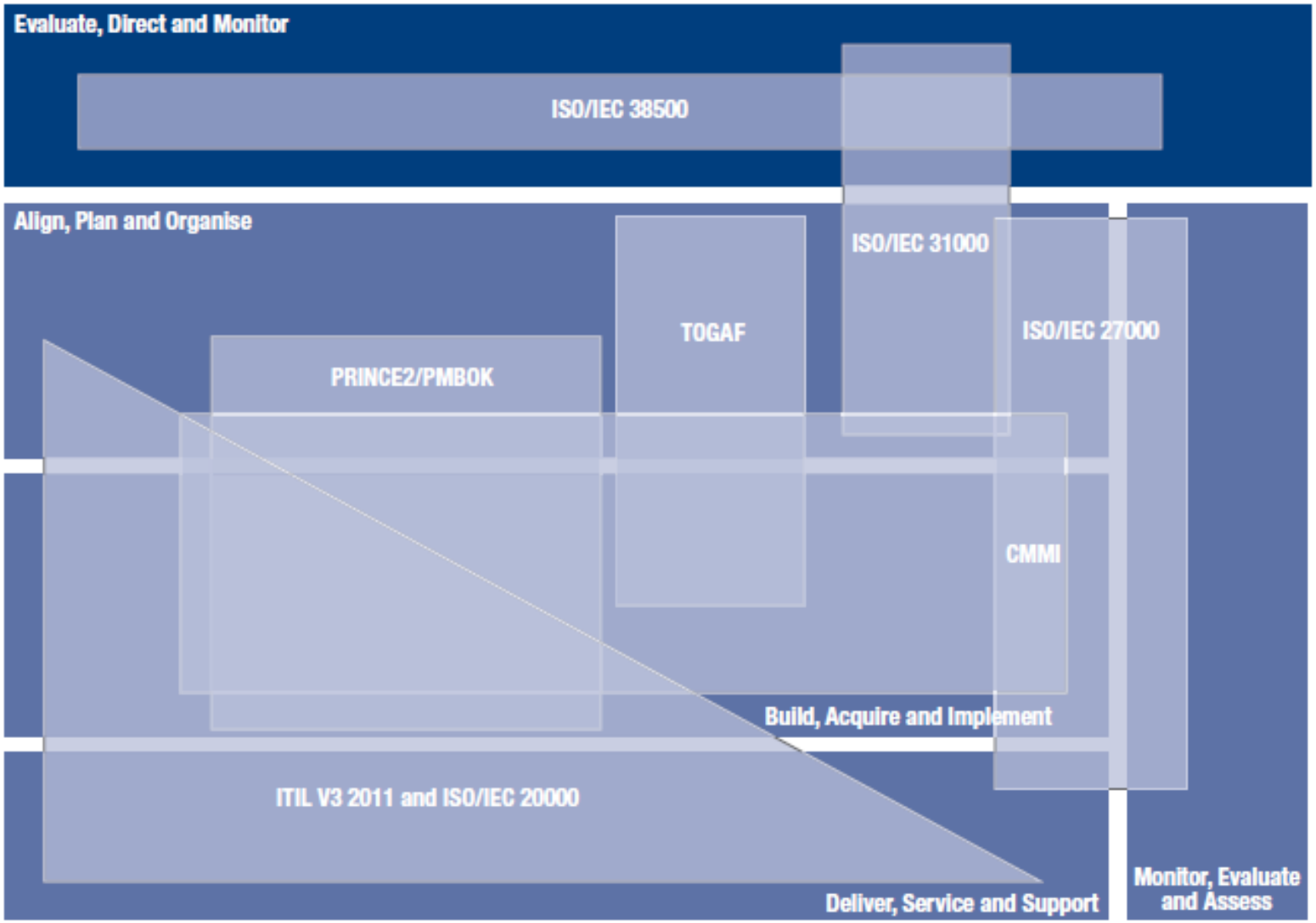
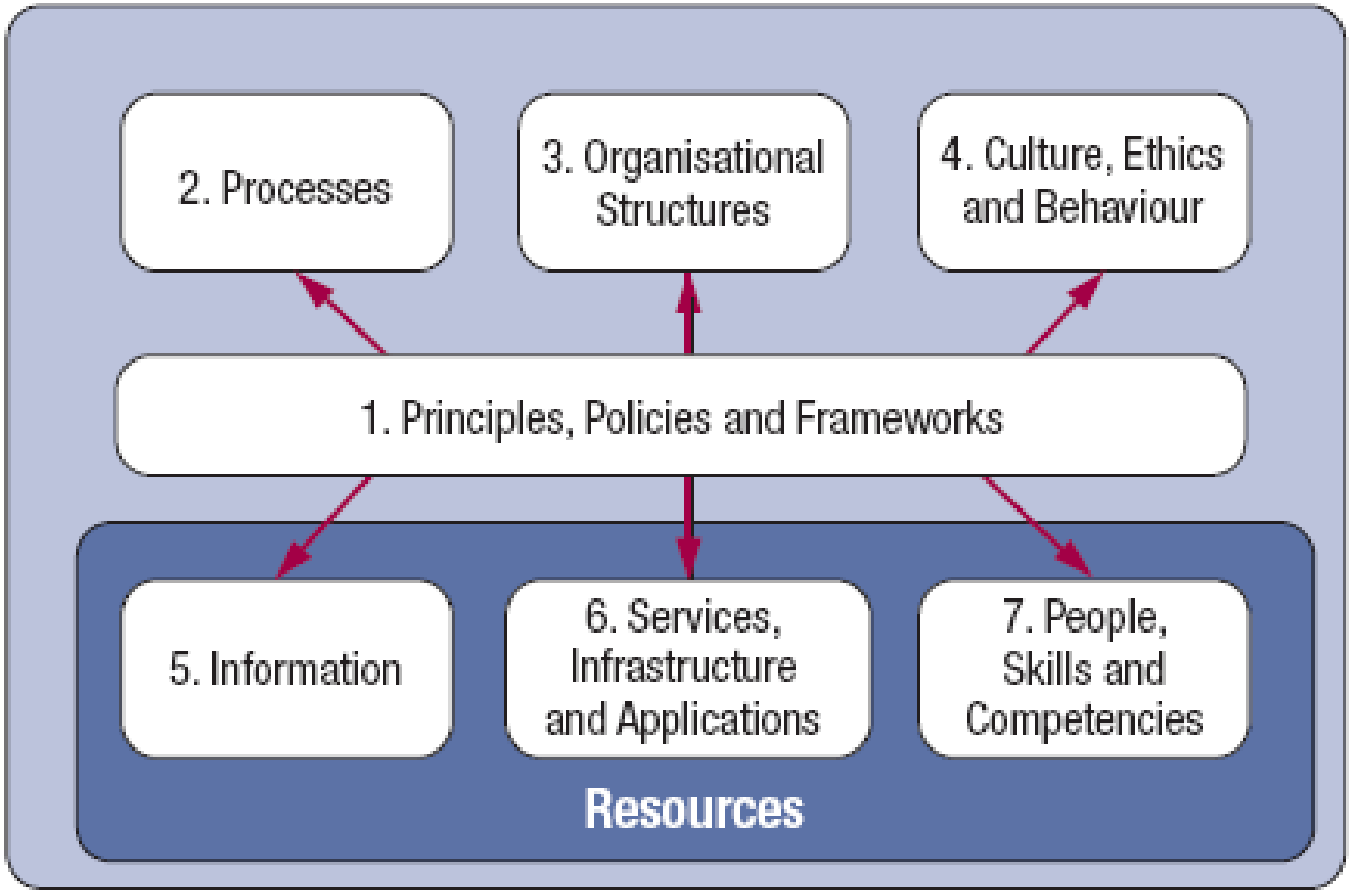


Figure 25—COBIT 5 Coverage of Other Standards and Frameworks



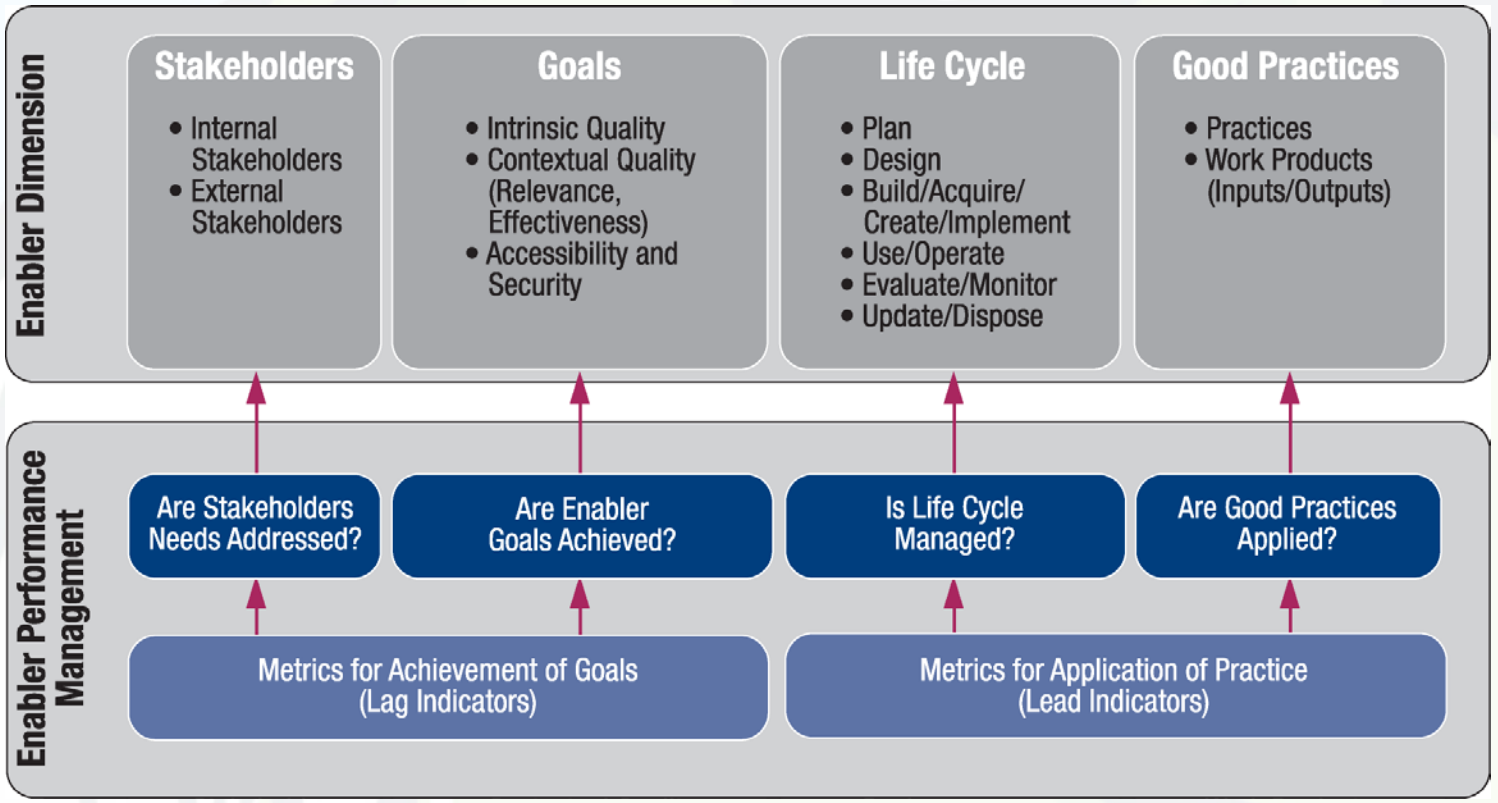
Enabling a Holistic Approach

COBIT 5 Enablers



COBIT 5 Enabler Dimensions

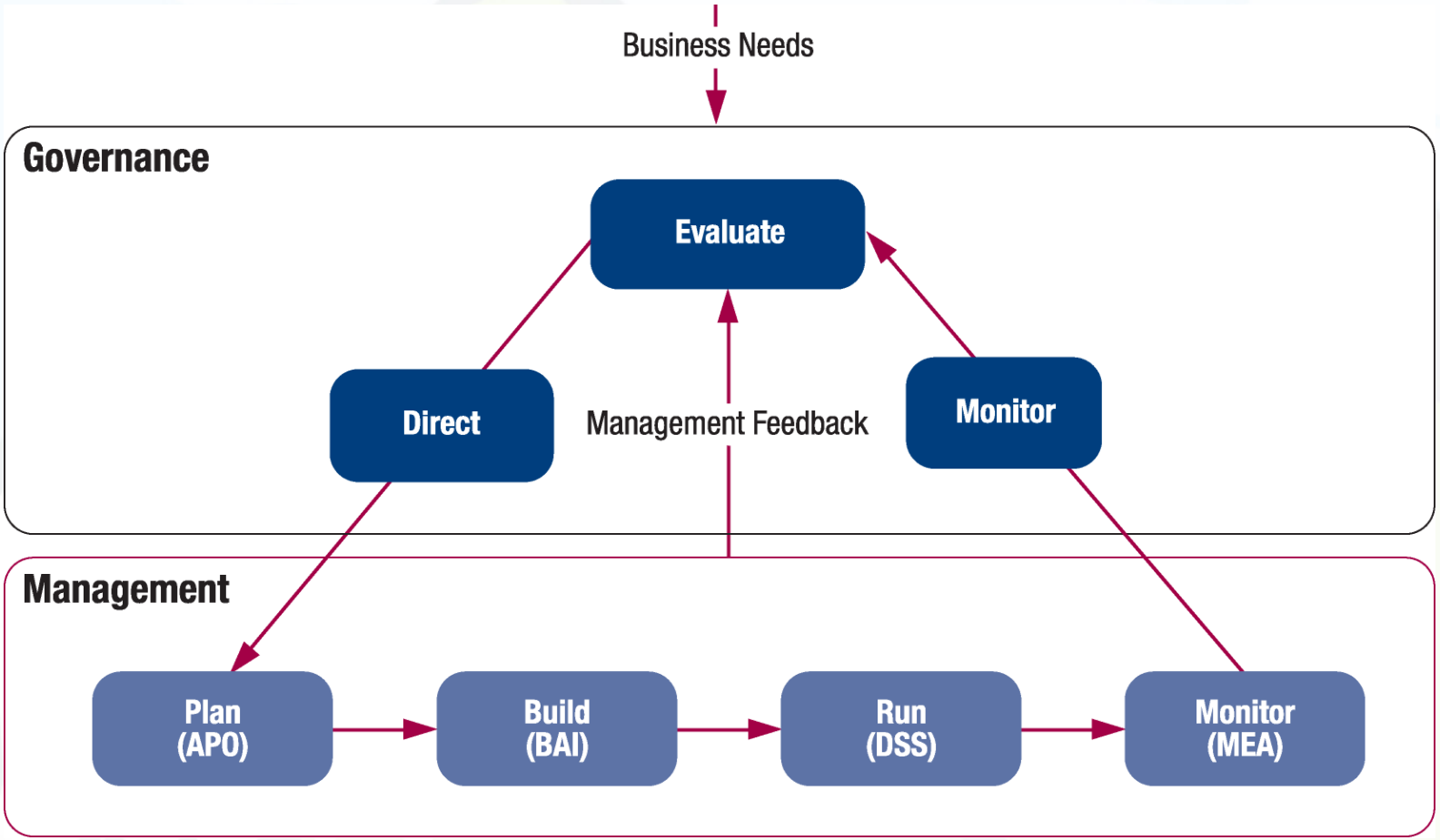
- All enablers have a set of common dimensions that:
  - Provide a common, simple and structured way to deal with enablers
  - Allow an entity to manage its complex interactions
  - Facilitate successful outcomes of the enablers



Governance and Management

- **Governance** ensures that stakeholder needs, conditions and options are **evaluated** to determine balance, agreed-on enterprise objectives to be achieved; setting **direction** through prioritisation and decision making; and **monitoring** performance, compliance and compliance against agreed-on direction and objectives (**EDM**).
- **Management plans, builds, runs** and **monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (**PBRM**).

Governance and Management



In Summary …

COBIT 5 brings together the **five principles** that allow the enterprise to build an effective **governance** and **management** framework based on a holistic set of **seven enablers** that optimises **information** and **technology** investment and use for the benefit of stakeholders.

COBIT 5 FOR RISK

FAQ (1 of 3)

- **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

FAQ (2 of 3)

- **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
- **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 best to use these example scenarios

FAQ (3 of 3)

- **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 FOR RISK

1. UNDERSTAND THE DRIVERS, BENEFITS AND TARGET AUDIENCES FROM A RISK PERSPECTIVE.

Drivers for Risk

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 appropriate 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

To achieve these aims, the *COBIT 5 for Risk* professional guide 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 of the alignment of *COBIT 5 for Risk* with other relevant standards

Benefits of the Guidance

- 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

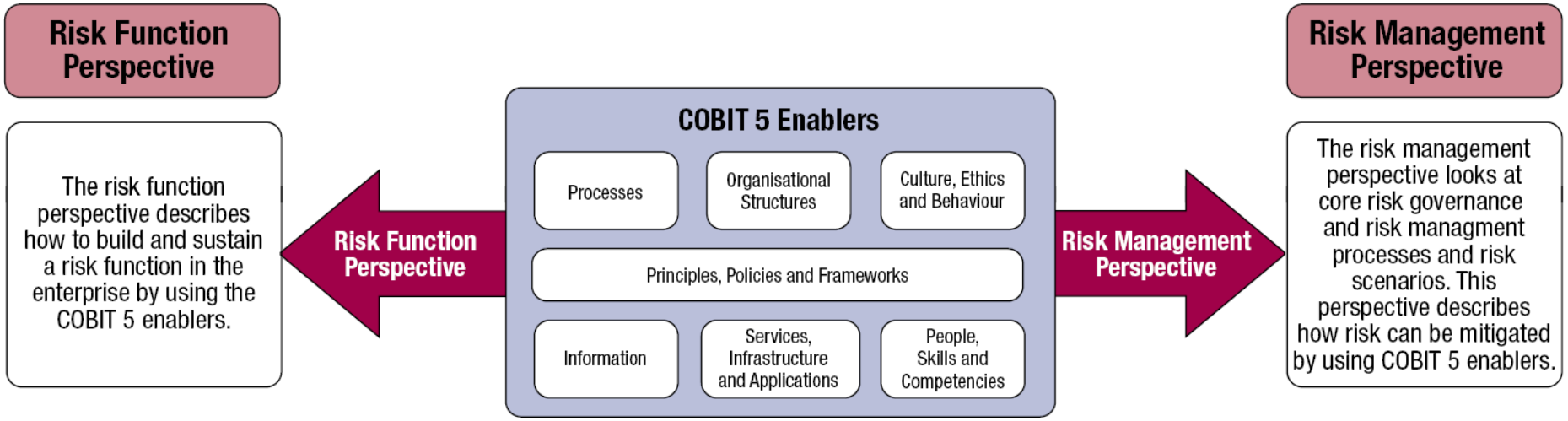
Target Audiences

- 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

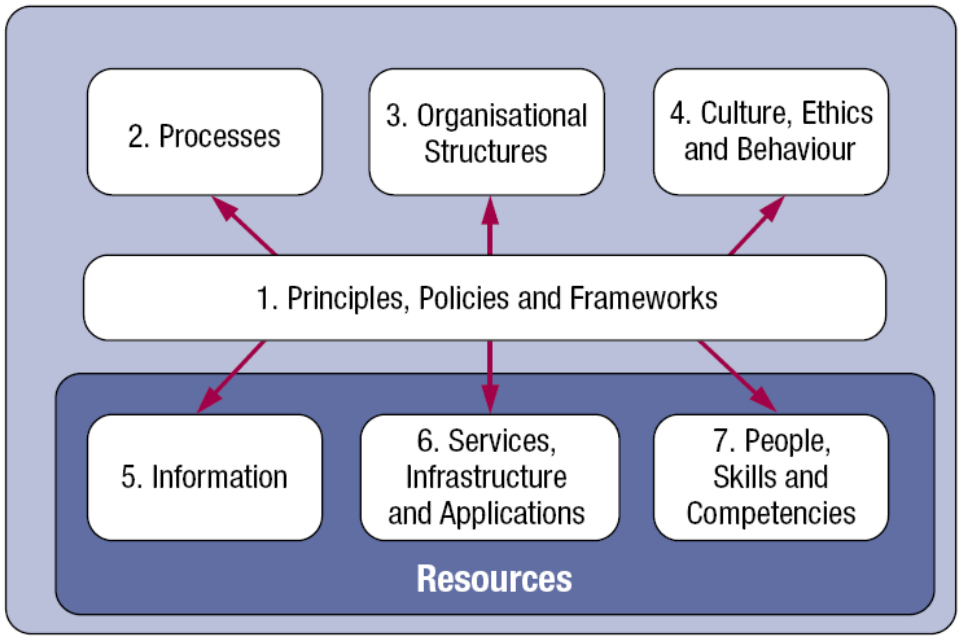
COBIT 5 FOR RISK

2. UNDERSTAND THE COMPONENTS OF RISK ACTIVITIES.

Risk Perspectives



Risk Function Perspective



COBIT 5 for Risk provides guidance and describes 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
- The **Organisational Structures** that are required to govern and manage risk effectively—e.g., enterprise risk committee, risk function
- What **People and Skills** should be put in place to establish and operate an effective risk function

Risk Function Perspective

COBIT 5 for Risk defines seven risk principles 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.

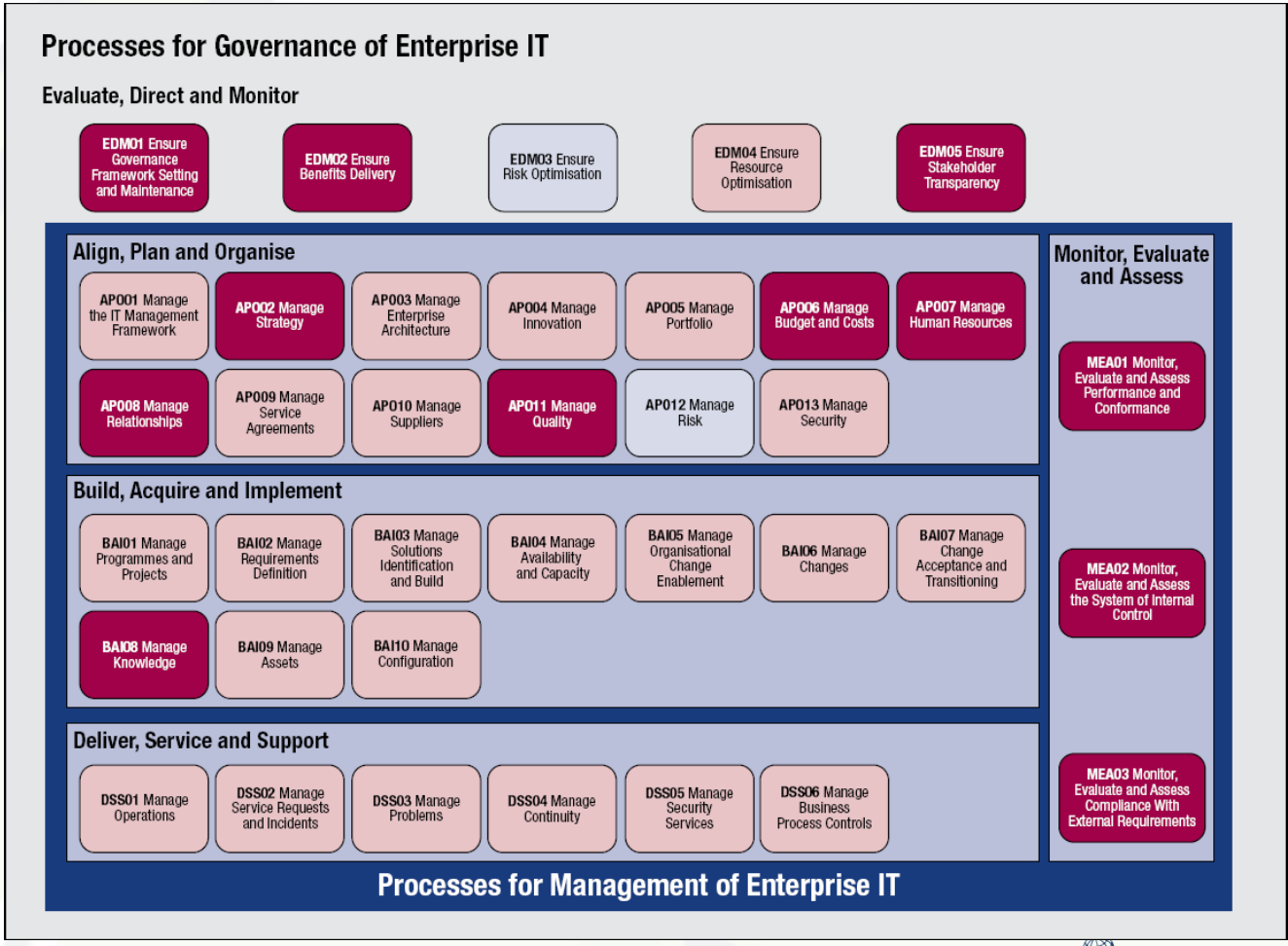
Risk Function Perspective

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.



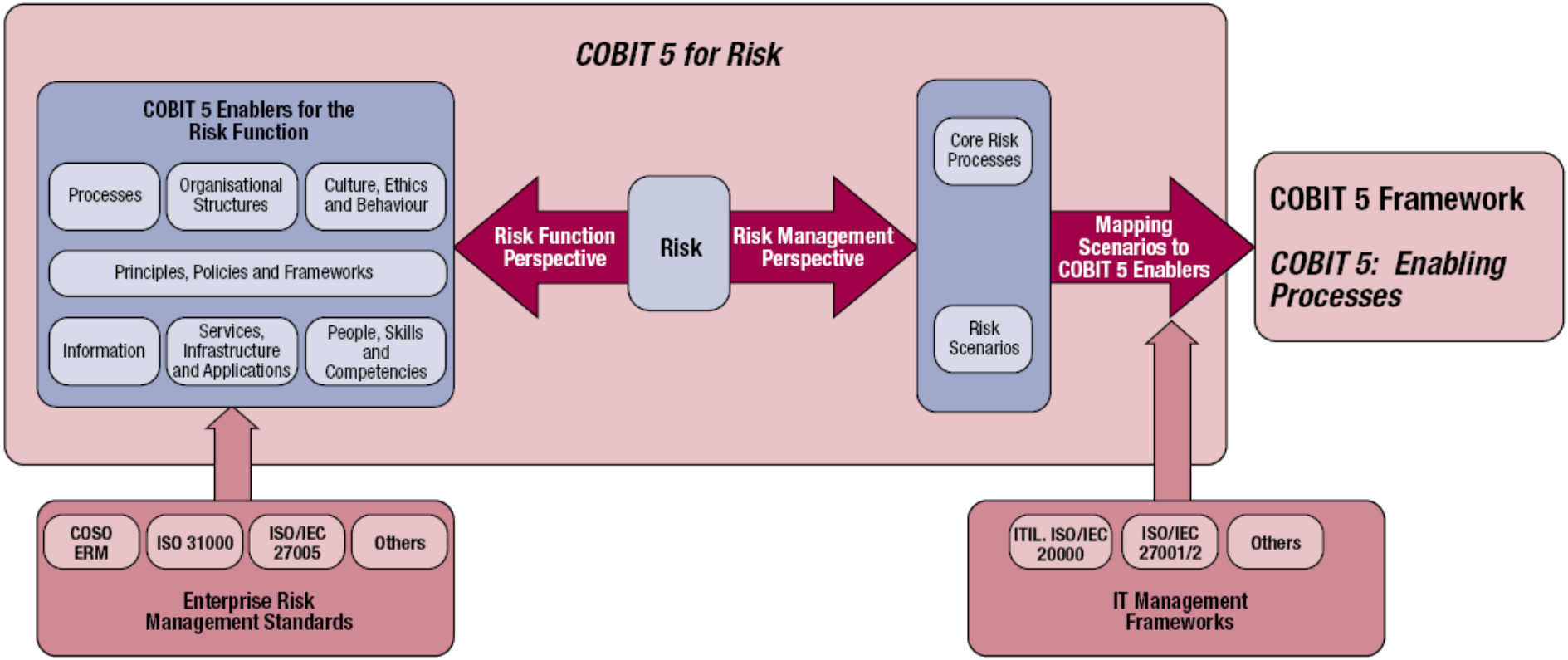
Risk Management Perspective

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 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 FOR RISK

3. UNDERSTAND HOW TO USE RISK SCENARIOS FOR GEIT.

Risk Scenarios

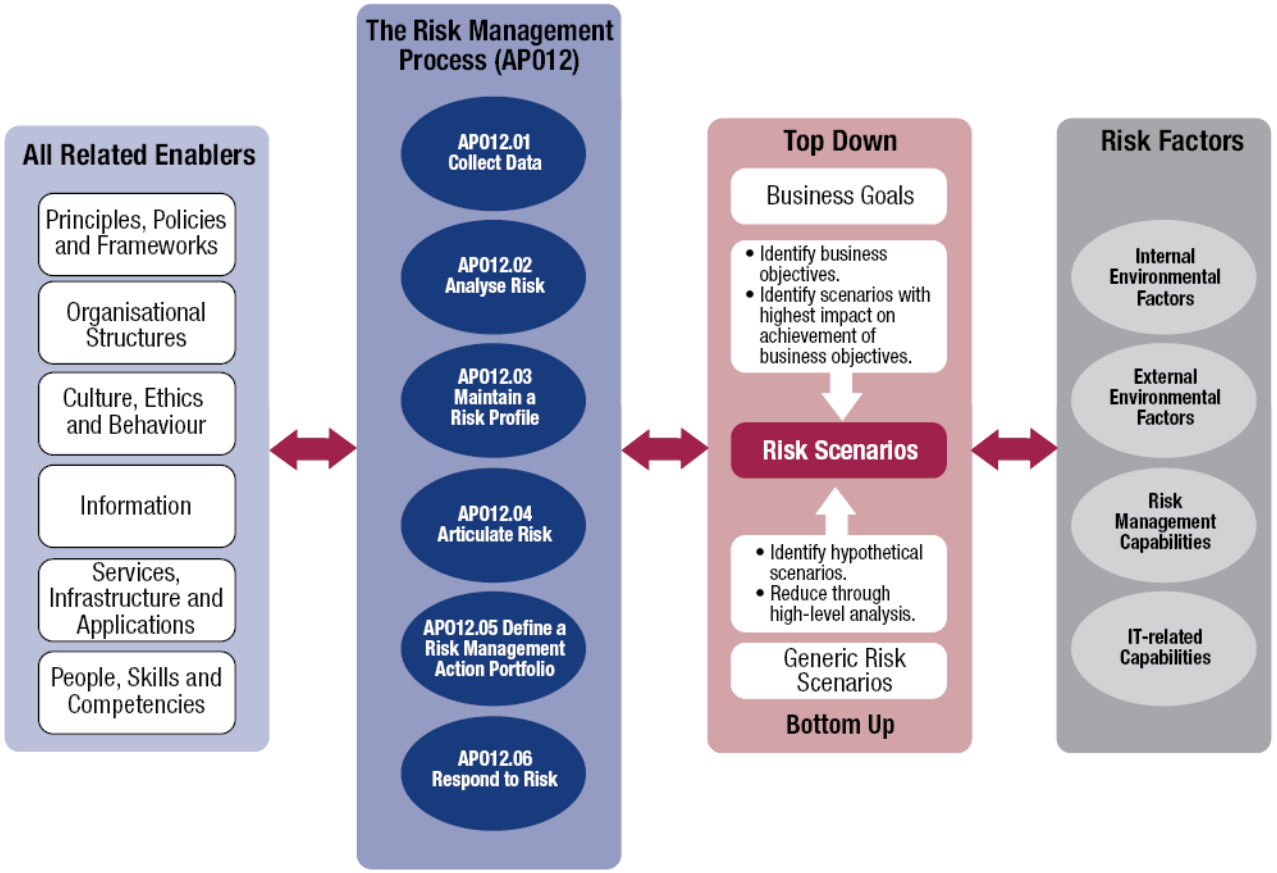
Definition

"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."

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

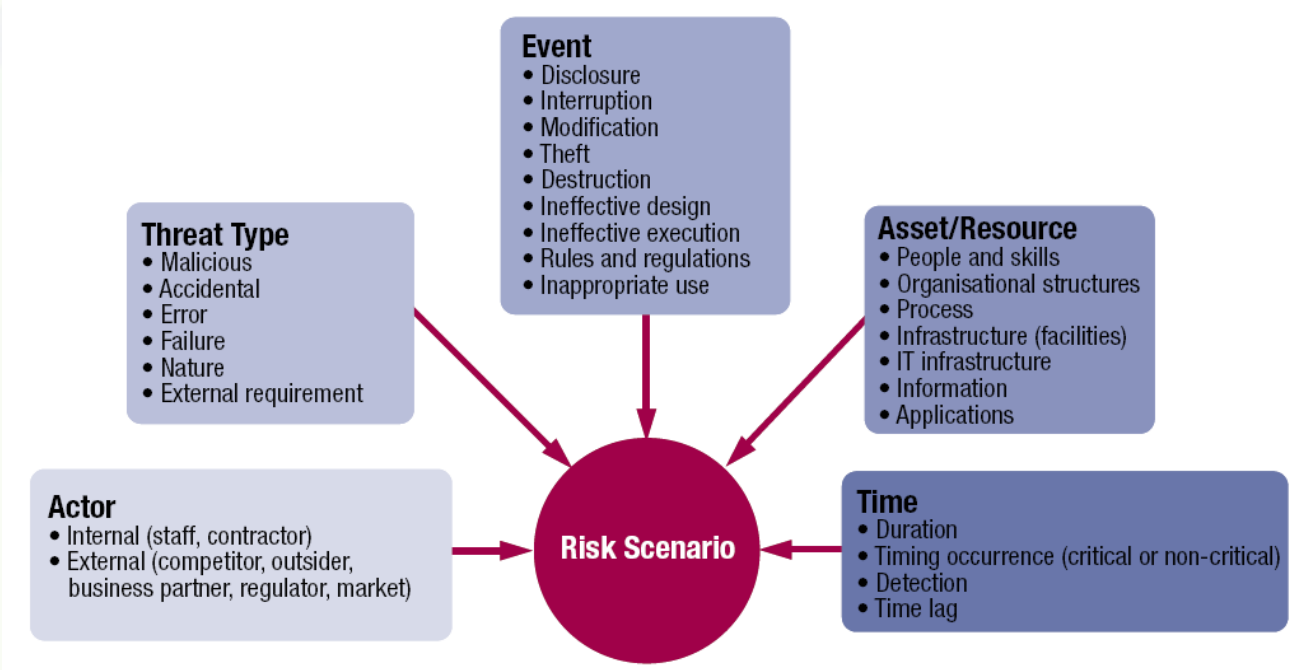


Risk Scenarios

- 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.

Risk Scenarios

When a risk scenario materialises, a loss event occurs. The loss event has been triggered by a threat event (Threat type + Event). The frequency of the threat event is influenced by a vulnerability. The vulnerability is usually a state; it can be increased/ decreased by vulnerability events, e.g., controls strength or by the threat strength.



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).	

Risk Response

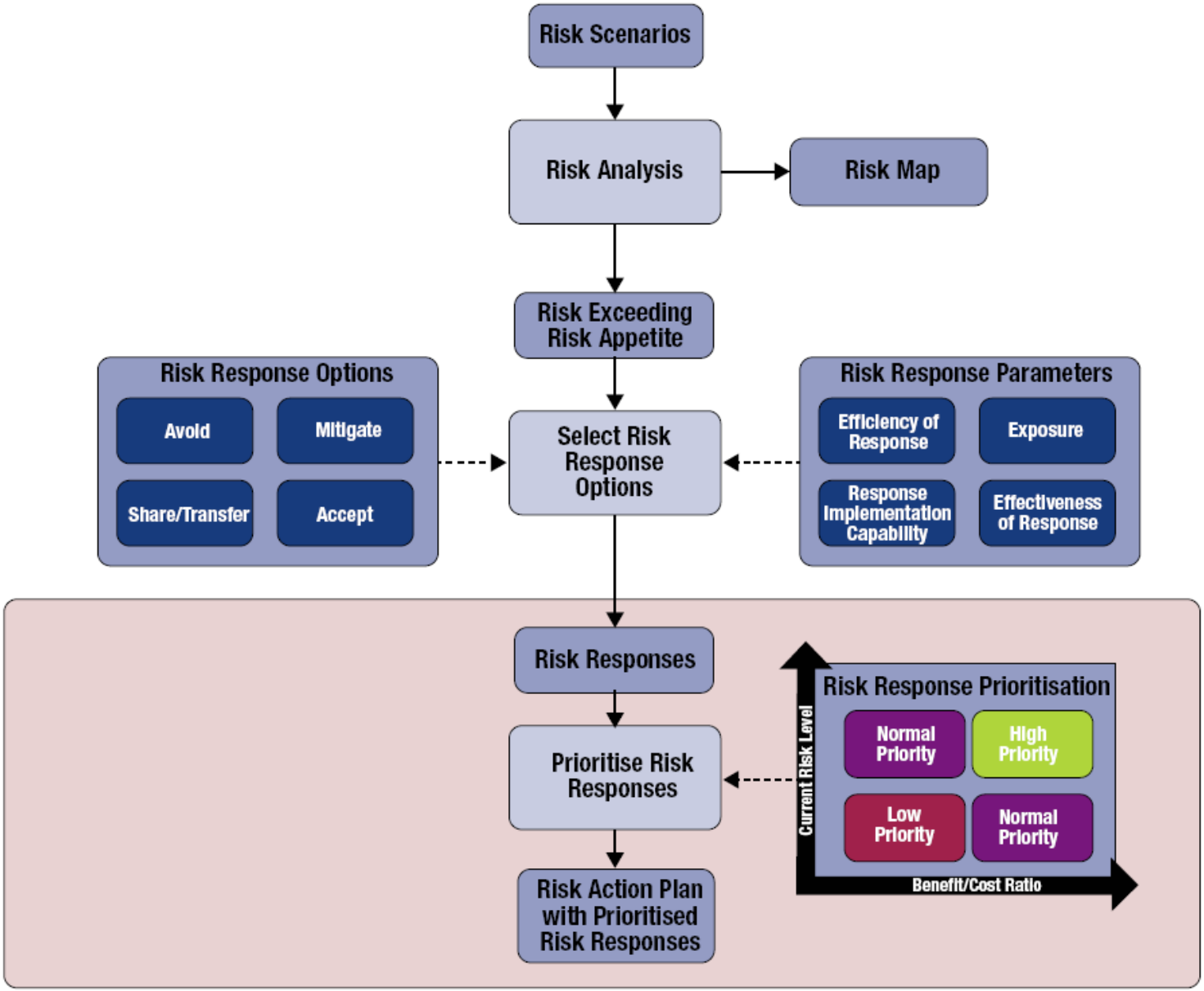
To bring risk in line with the risk appetite for the enterprise:

- 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.

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.
- 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.

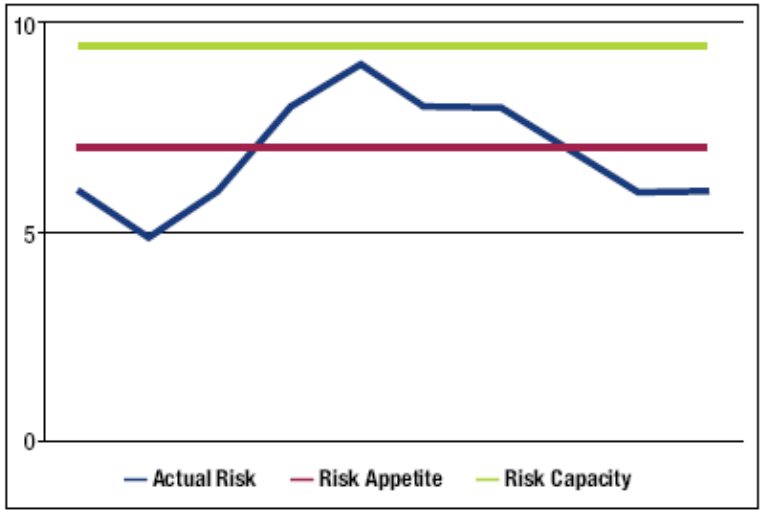
D.3. Scenario 3: IT Investment Decision Making		
Risk Scenario Category	IT investment decision making	
Principles, Policies and Frameworks Enabler		
Reference	**Contribution to Response to Scenario**	
Programme/Project management policy	The policy should define who needs to be involved in investment decisions and the chain of approval.	
Process Enabler		
Reference	**Title**	**Management Practice**
AP005.06	Manage benefits achievement.	Monitor the benefits of providing and maintaining appropriate IT services and capabilities, based on the agreed-on and current business case.
AP006.02	Prioritise resource allocation.	Implement a decision-making process to prioritise the allocation of resources and rules for discretionary investments by individual business units. Include the potential use of external service providers and consider the buy, develop and rent options.
AP006.03	Create and maintain budgets.	Prepare a budget reflecting the investment priorities supporting strategic objectives based on the portfolio of IT-enabled programmes and IT services.
AP007.01	Maintain adequate and appropriate staffing.	Evaluate staffing requirements on a regular basis or on major changes to the enterprise or operational or IT environments to ensure that the enterprise has sufficient human resources to support enterprise goals and objectives. Staffing includes both internal and external resources.
BAI01.03	Manage stakeholder engagement.	Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information that reaches all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.
BAI03.04	Procure solution components.	Procure solution components based on the acquisition plan in accordance with requirements and detailed designs, architecture principles and standards, and the enterprise's overall procurement and contract procedures, QA requirements, and approval standards. Ensure that all legal and contractual requirements are identified and addressed by the supplier.

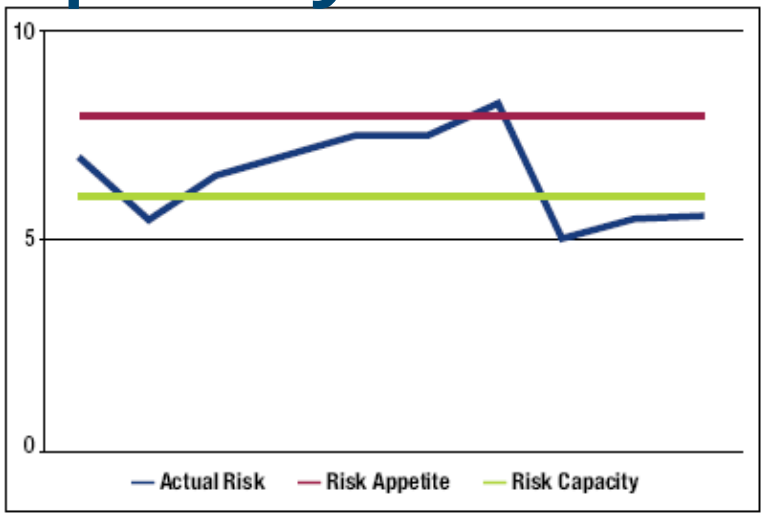

Risk Scenarios
Risk Analysis
Risk Map
Risk Exceeding Risk Appetite
Risk Response Options
Avoid
Mitigate
Share/Transfer
Accept
Select Risk Response Options
Risk Response Parameters
Efficiency of Response
Exposure
Response Implementation Capability
Effectiveness of Response
Risk Responses
Prioritise Risk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

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 about 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 situation

COBIT 5 FOR RISK

4. UNDERSTAND HOW *COBIT 5 FOR RISK* RELATES TO AND ALIGNS WITH 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
  - ISO 27005:2011 – Information security risk management
  - COSO Enterprise Risk Management

Alignment

- ISO 31000:2009 – Risk Management
  - *COBIT 5 for Risk* **addresses all** ISO 31000 principles, through the:
    - *COBIT 5 for Risk* principles and enablers themselves
    - Enabler models
  - In addition, the framework and process model aspects are covered in greater detail by the *COBIT 5 for Risk* process model.
  - All elements are included in *COBIT 5 for Risk* and are often expanded on or elaborated in greater detail, specifically for IT risk management.

Alignment

- ISO 27005:2011 – Information security risk management
  - *COBIT 5 for Risk* **addresses all** of the components described within ISO 27005. Some of the elements are structured or named differently.
  - *COBIT 5 for Risk* **takes a broader view** on IT risk management compared with ISO 27005 which is focused on the management of security related risk.
  - There is a **stronger emphasis** in *COBIT 5 for Risk* on processes and practices to ensure the alignment with business objectives, the acceptance throughout the organisation and the completeness of the scope, amongst other factors.

Alignment

- COSO Enterprise Risk Management
  - *COBIT 5 for Risk* **addresses all** of the components defined in COSO ERM.
  - Although *COBIT 5 for Risk* focuses less on control, it provides **linkages to enablers—**management practices in the COBIT 5 framework.
  - The **essentials with regards to both control and general risk management** as defined in COSO ERM are present in *COBIT 5 for Risk*, either through the:
    - Principles themselves and the framework's conceptual design
    - Process model and additional guidance provided in the framework

Thank You for Attending!

Presented by: Nelson Gibbs
CIA, CRMA, CISA, CISM, CGEIT, CRISC, CISSP
ngibbs@pacbell.net

Questions???