# COBIT 5 FOR
# IT RISK MANAGEMENT

Prof. dr. Wim Van Grembergen
University of Antwerp (UA)
IT Alignment and Governance (ITAG) Research Institute
wim.vangrembergen@ua.ac.be

ISACA®
Trust in, and value from, information systems

# COBIT® 5

## *for Risk*

COBIT® 5
AN ISACA® FRAMEWORK

## AGENDA

- COBIT 5 overview
- IT risk defined
- Risk function perspective
- Risk management perspective
- Risk scenarios

-

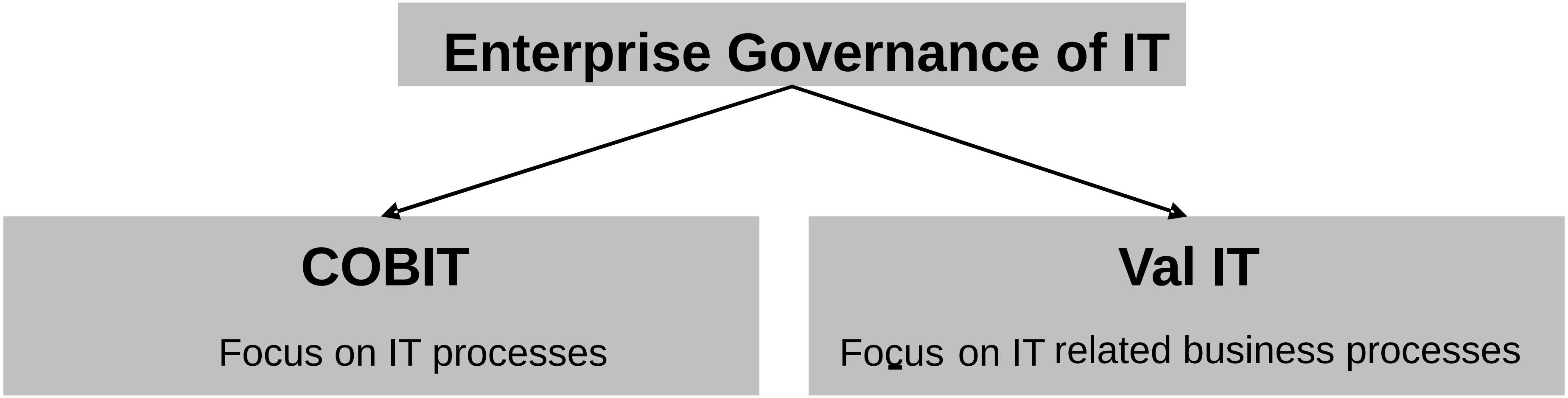
# COBIT 5 overview

## Enterprise Governance of IT

Enterprise governance of IT (EGIT) is an integral part of enterprise governance exercised by the Board overseeing the definition and implementation of processes, structures and relational mechanisms in the organisation enabling both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments.

(Van Grembergen & De Haes, 2009 and 2015)

# COBIT and VALIT as frameworks for Enterprise Governance of IT



Enterprise Governance of IT

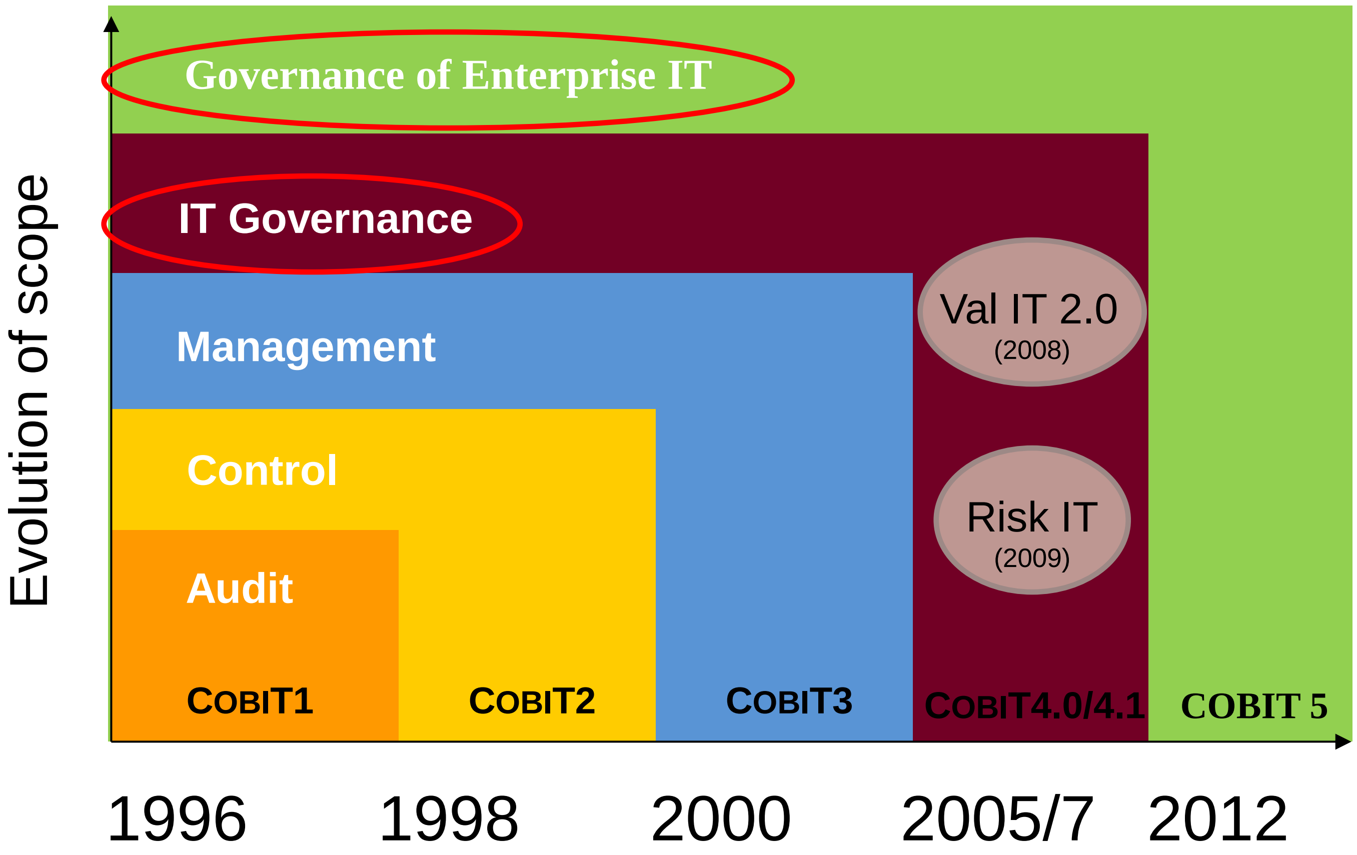
COBIT

Focus on IT processes

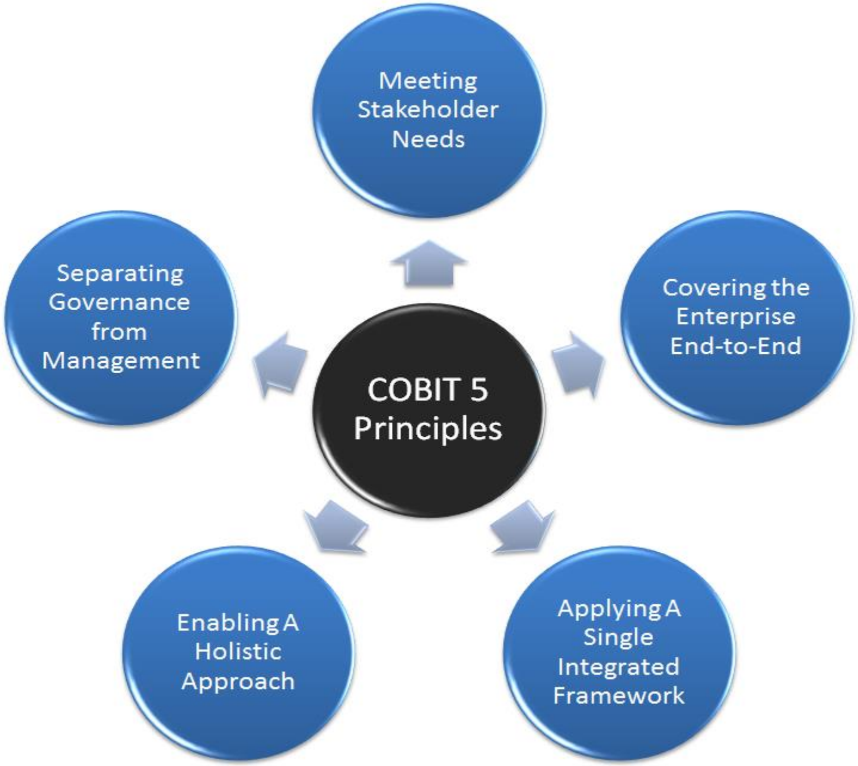
Val IT

Focus on IT related business processes

# COBIT evolution



# COBIT 5



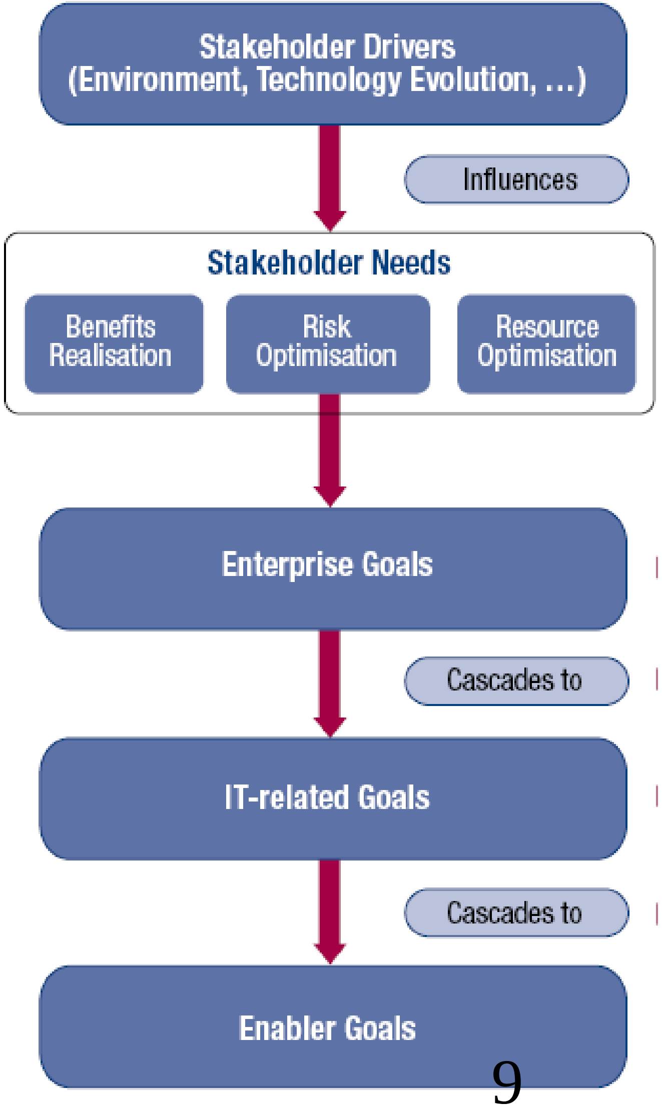
Meeting Stakeholder Needs
Covering the Enterprise End-to-End
Applying A Single Integrated Framework
Enabling A Holistic Approach
Separating Governance from Management
COBIT 5 Principles

**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.

# 1. Meeting stakeholder needs

Stakeholder needs have to be transformed into an enterprise’s actionable strategy.

The COBIT 5 goals cascade translates stakeholder needs into specific, actionable and customised goals within the context of the enterprise, IT-related goals and enabler goals.



# 2. Covering the Enterprise End-to-end

| KMP REF | Practice | Board | CEO | CFO | COO | Business Executives | Business Process Owners | Strategy (exec) Commitee | Steering (Programmes / Projects) Com | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Commitee | HR | Compliance Audit | CIO | Head Architect | Head Development | Head IT Operations | Head IT Administration | Project Management Office | Service Manager | Information Security Manager | Bus_Cont_ Manager | Privacy Officer |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DSS04.01 | Define incident and request fulfilment classification schemes | | | | | | C | | | | | | | | | A | R | R | R | | | R | C | | C |
| DSS04.02 | Record, classify and prioritise requests and incidents | | | | | | I | | | | | | | | | | | | A | | | I | | | I |
| DSS04.03 | Verify, approve and fulfil service requests | | | | | | R | | | | | | | | | I | R | R | R | | | A | | | |
| DSS04.04 | Investigate, diagnose and escalate incidents | | | | | | I | | | | | | | | | I | | C | A | | | I | C | | |
| DSS04.05 | Resolve and recover incidents | | | | | | I | | | | | | | | | I | | R | R | | | A | R | | C |
| DSS04.06 | Close service requests and incidents | | | | | | I | | | | | | | | | I | | I | A | | | I | R | | |
| DSS04.07 | Track status and produce reports | | | | | | I | | | | | | | | | I | | I | I | | | I | I | | |

# 3. Applying a Single Integrated Framework

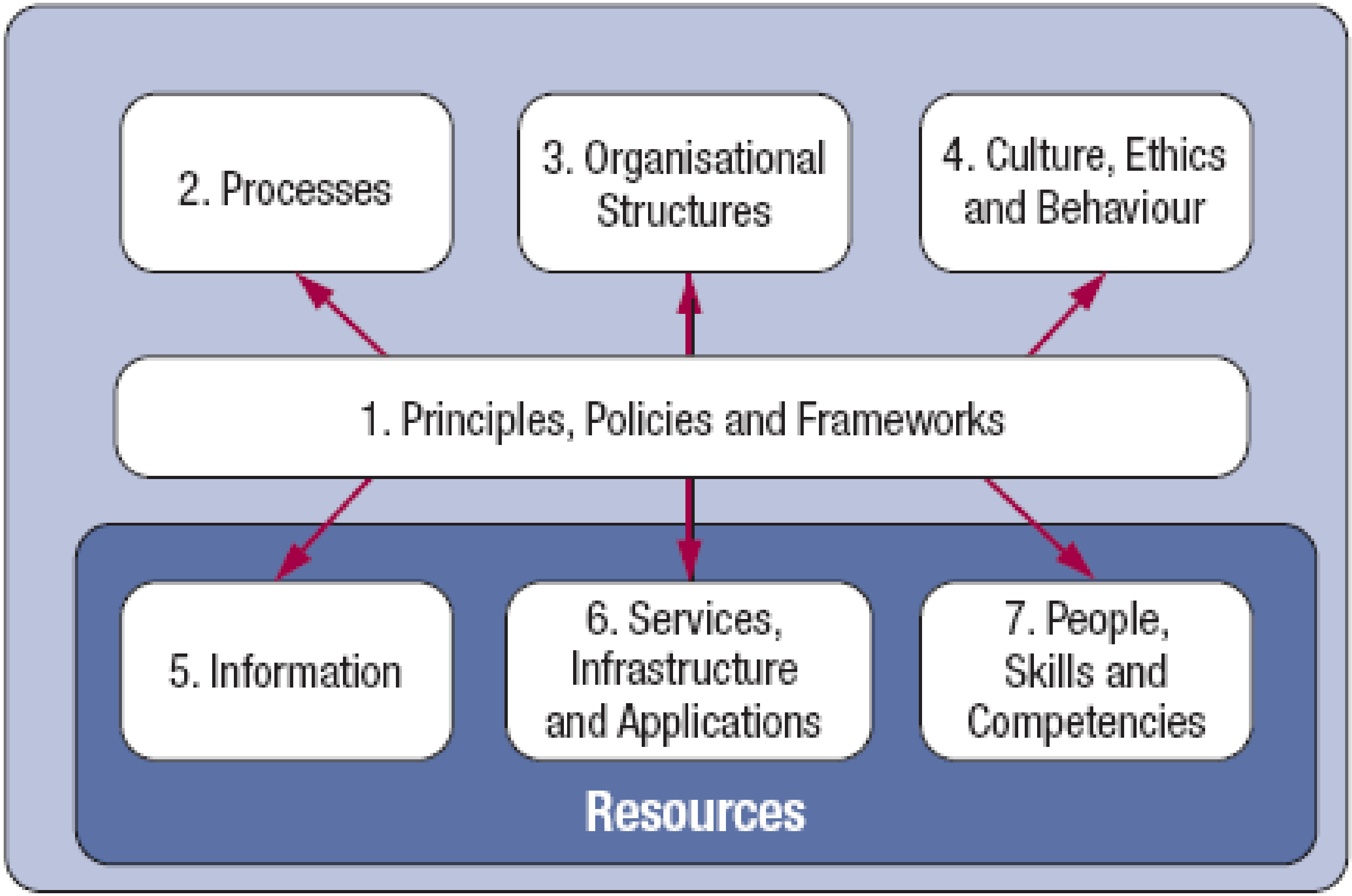
COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises:

- Enterprise: COSO, COSO ERM, ISO/IEC 9000, **ISO/IEC 31000**
- IT-related: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOK/PRINCE2, CMMI
- Etc.

This allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.

ISACA plans a capability to facilitate COBIT user mapping of practices and activities to third-party references.

## 4. Enabling a Holistic Approach

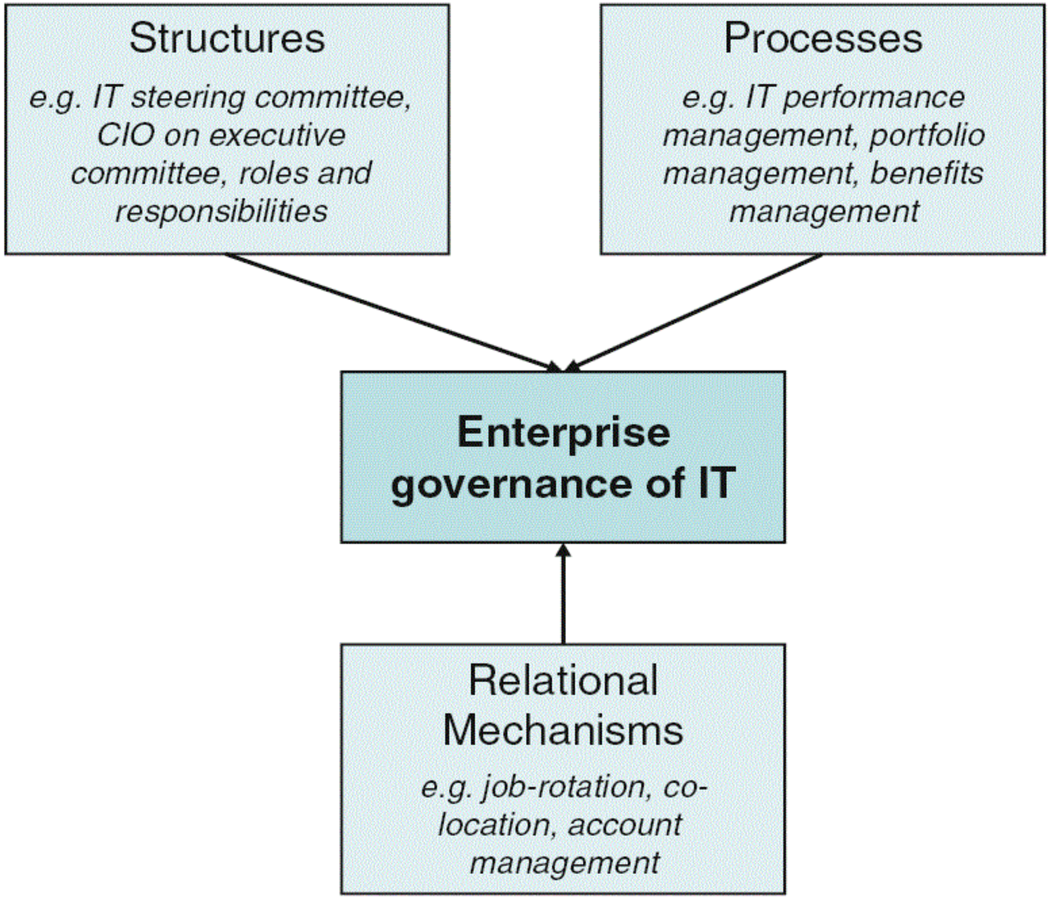


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

# Principle 4: Enabling a holistic approach (continued)

- EGIT research (Van Grembergen and De Haes) shows that organizations can deploy EGIT by using a mixture of various structures, processes, and relational mechanisms
- COBIT 5 builds on these insights and incorporates the “enablers” in its framework

# IT GOVERNANCE MODEL
## (Van Grembergen – De Haes)



Structures

*e.g. IT steering committee, CIO on executive committee, roles and responsibilities*

Processes

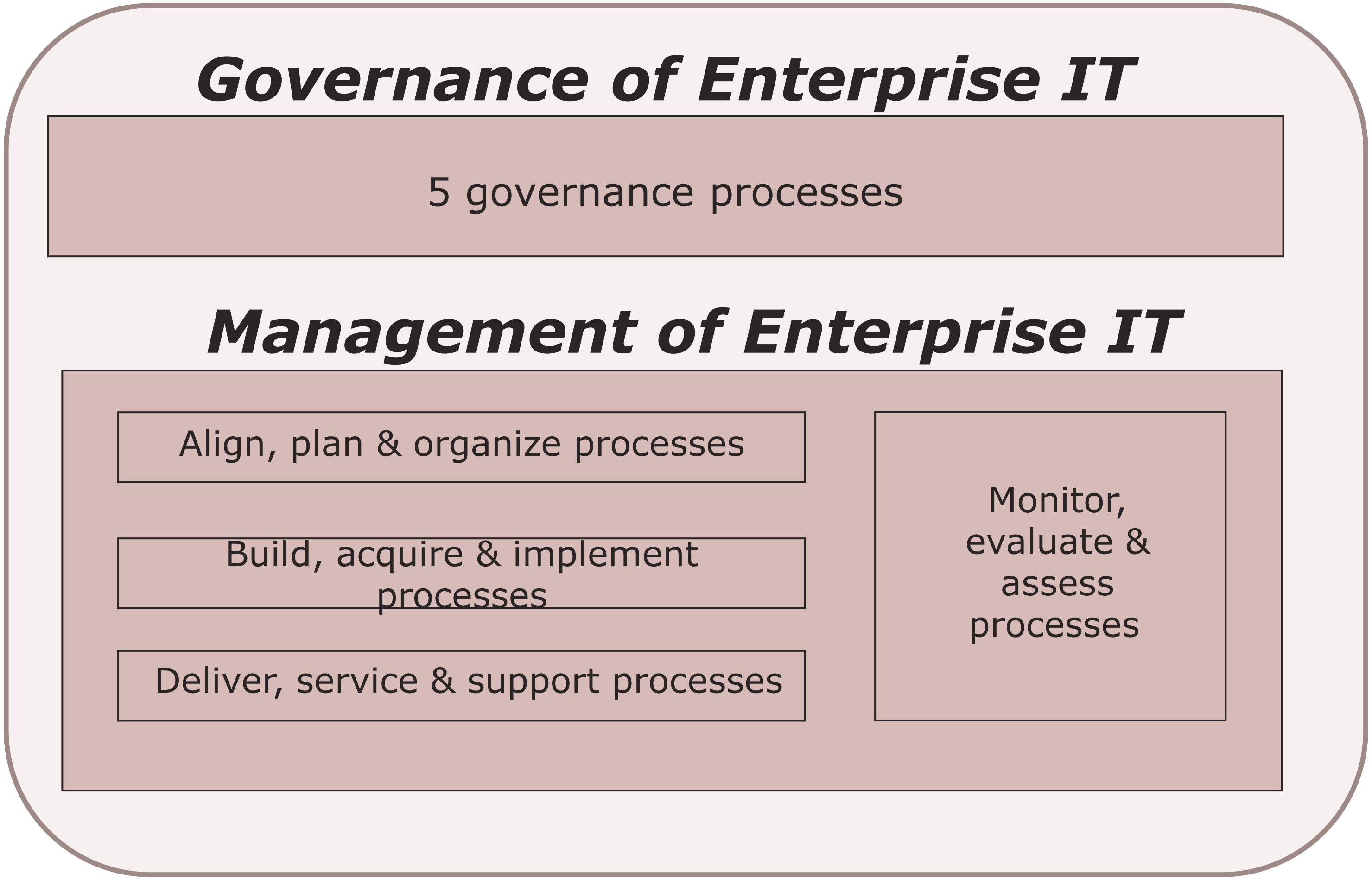
*e.g. IT performance management, portfolio management, benefits management*

**Enterprise governance of IT**

Relational Mechanisms

*e.g. job-rotation, co-location, account management*

# 5. Separating Governance From Management



***Governance of Enterprise IT***

5 governance processes

***Management of Enterprise IT***

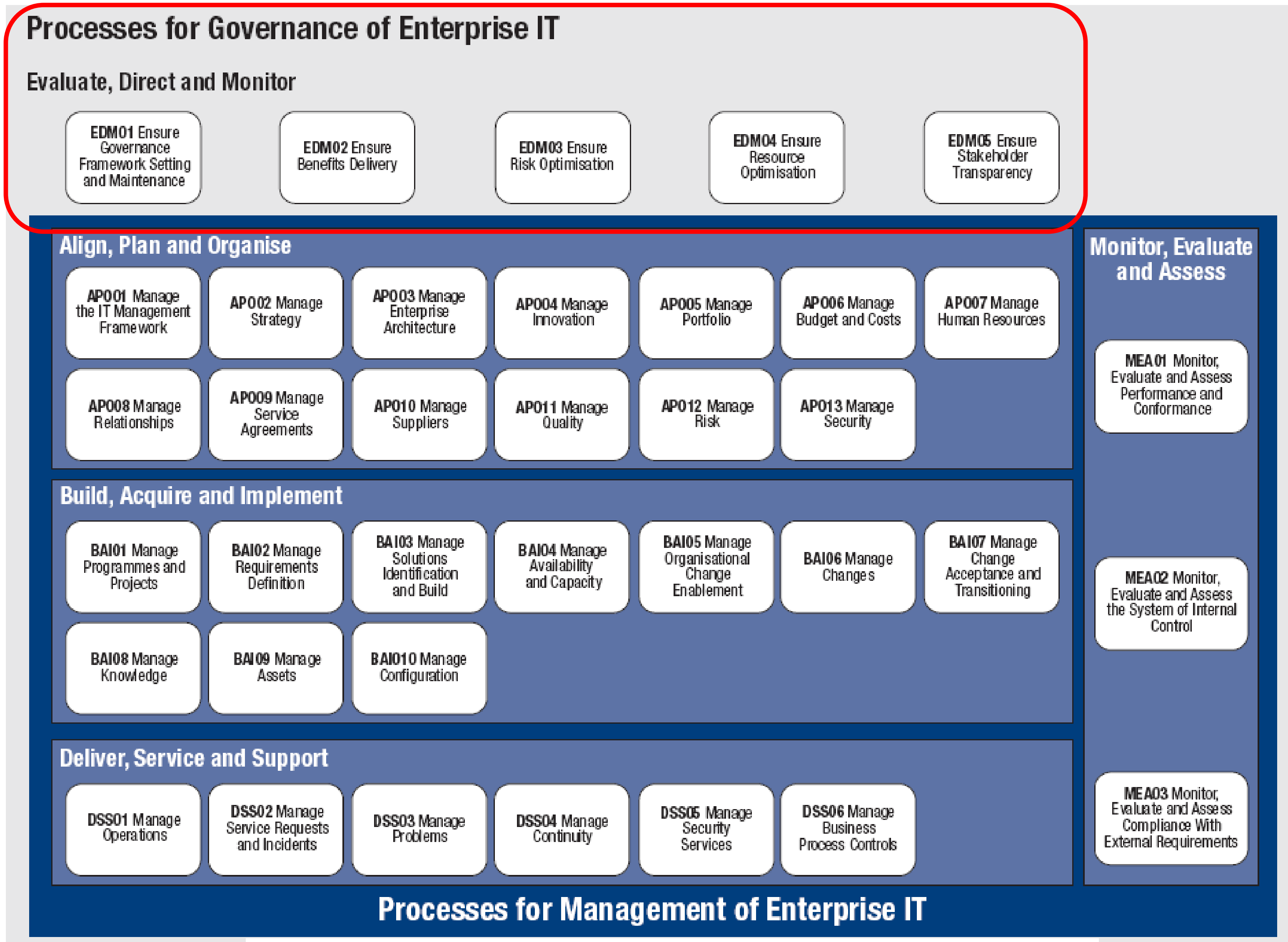
Align, plan & organize processes

Build, acquire & implement processes

Deliver, service & support processes

Monitor, evaluate & assess processes

# Governance in COBIT 5



## Processes for Governance of Enterprise IT

### Evaluate, Direct and Monitor

- **EDM01** Ensure Governance Framework Setting and Maintenance
- **EDM02** Ensure Benefits Delivery
- **EDM03** Ensure Risk Optimisation
- **EDM04** Ensure Resource Optimisation
- **EDM05** Ensure Stakeholder Transparency

### Align, Plan and Organise

- **APO01** Manage the IT Management Framework
- **APO02** Manage Strategy
- **APO03** Manage Enterprise Architecture
- **APO04** Manage Innovation
- **APO05** Manage Portfolio
- **APO06** Manage Budget and Costs
- **APO07** Manage Human Resources
- **APO08** Manage Relationships
- **APO09** Manage Service Agreements
- **APO10** Manage Suppliers
- **APO11** Manage Quality
- **APO12** Manage Risk
- **APO13** Manage Security

### Build, Acquire and Implement

- **BAI01** Manage Programmes and Projects
- **BAI02** Manage Requirements Definition
- **BAI03** Manage Solutions Identification and Build
- **BAI04** Manage Availability and Capacity
- **BAI05** Manage Organisational Change Enablement
- **BAI06** Manage Changes
- **BAI07** Manage Change Acceptance and Transitioning
- **BAI08** Manage Knowledge
- **BAI09** Manage Assets
- **BAI010** Manage Configuration

### Deliver, Service and Support

- **DSS01** Manage Operations
- **DSS02** Manage Service Requests and Incidents
- **DSS03** Manage Problems
- **DSS04** Manage Continuity
- **DSS05** Manage Security Services
- **DSS06** Manage Business Process Controls

### Monitor, Evaluate and Assess

- **MEA01** Monitor, Evaluate and Assess Performance and Conformance
- **MEA02** Monitor, Evaluate and Assess the System of Internal Control
- **MEA03** Monitor, Evaluate and Assess Compliance With External Requirements

## Processes for Management of Enterprise IT

Source: COBIT® 5, figure 16. © 2012 ISACA® All rights reserved.

# IT RISK DEFINED

# IT RISK DEFINED

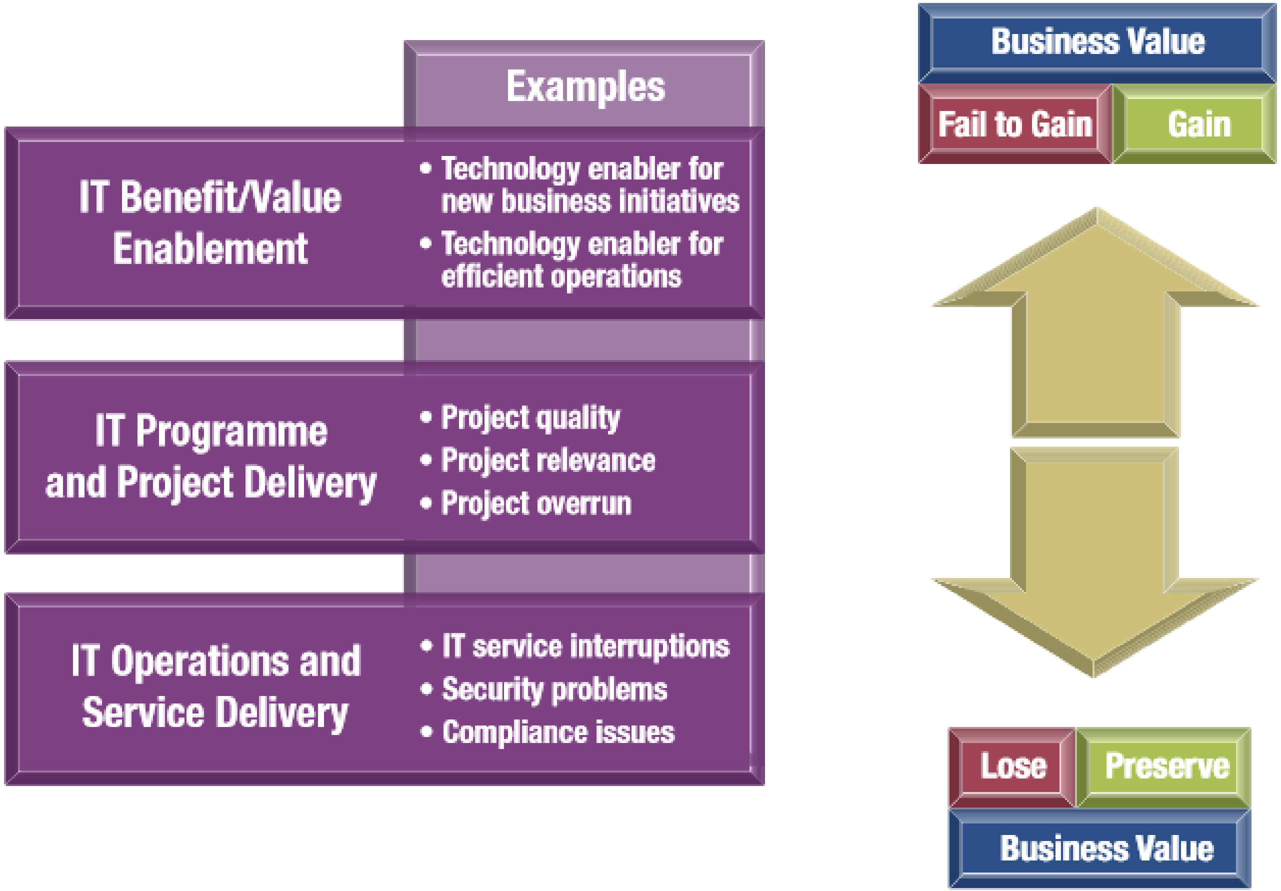
# Definition of risk

Risk can be defined as the combination of the probability of an event and its consecquences that enterprise objectives are not met.

COBIT 5 defines IT risk as business risk specifically the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

IT risk consists of IT-related events that potentially impact the business creating challenges in meeting strategic goals and objectives.

# IT risk categories



|  | Examples |
|---|---|
| IT Benefit/Value Enablement | • Technology enabler for new business initiatives<br>• Technology enabler for efficient operations |
| IT Programme and Project Delivery | • Project quality<br>• Project relevance<br>• Project overrun |
| IT Operations and Service Delivery | • IT service interruptions<br>• Security problems<br>• Compliance issues |

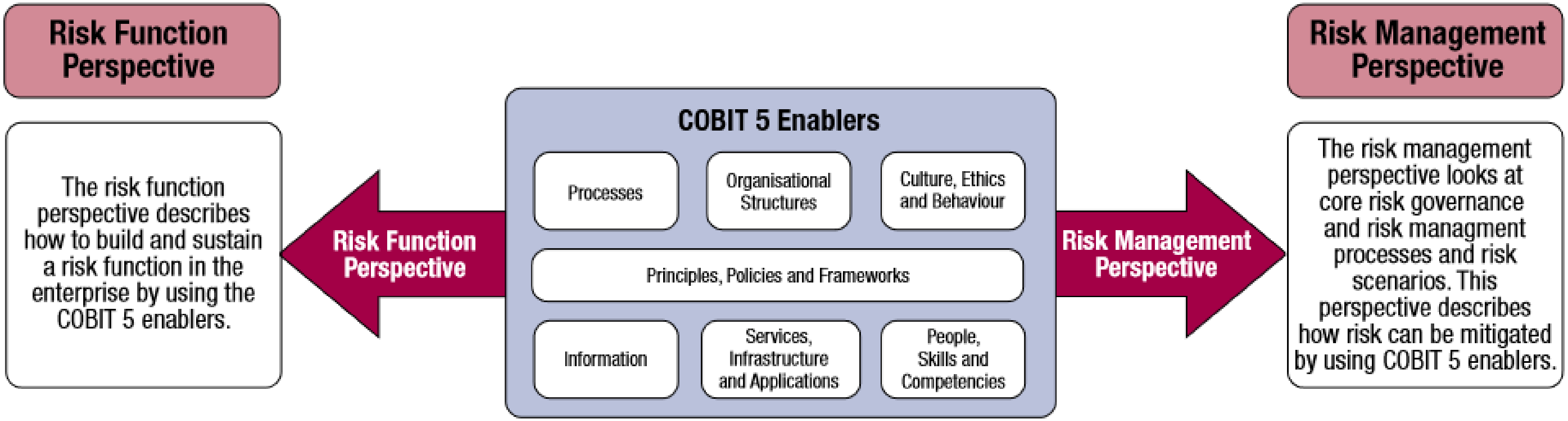
# Benefits Risk

- Non-alignment with commercial policies or strategy
- Non-alignment with technical standards, architecture, etc.
- Compliance with security guidelines/policy
- Clarity and credibility of desired business outcomes
- Measurability of outcomes (lead and lag indicators)
- Benefits monitoring processes
- Sensitivity of outcomes to timing or external dependencies, including changes in the economy, market conditions or a specific industry sector.
- Extent of organisational change required (depth and breadth)
- Clarity of the scope of organisational change required
- Quality of the change management plan
- Preparedness and capability of business to handle the change
- Level of business organisational understanding of and commitment to the programme
- Quality and availability of business sponsorship
- Senior business department staff engagement
- ‘Big bang’ programme or ‘do-able chunks’

# Delivery Risk

- Quality of the programme and project plans (completeness and reasonability)
- Clarity of scope and deliverables
- Unproven technology
- Compliance with technology architecture and standards
- Project duration
- Size of the project in relation to earlier successful projects
- Level of interface required to existing systems and processes
- Senior business department staff involvement
- Key staff availability during project deployment
- Experience/quality of project managers
- Experience/quality of project teams
- Reliance on vendors
- Dependency on factors outside control of project teams
- Quality of risk control mechanisms
- Ability to provide ongoing operational support

# TWO PERSPECTIVES ON RISK



**Risk Function Perspective**

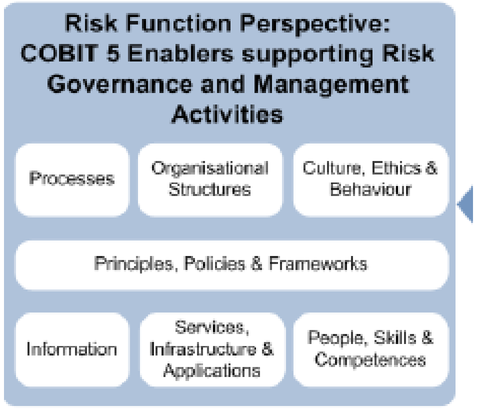
The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT 5 enablers.

**Risk Management Perspective**

The risk management perspective looks at core risk governance and risk managment processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.

Risk Function Perspective
COBIT 5 Enablers
Processes
Organisational Structures
Culture, Ethics and Behaviour
Principles, Policies and Frameworks
Information
Services, Infrastructure and Applications
People, Skills and Competencies
Risk Management Perspective

# RISK MANAGEMENT PERSPECTIVE



Risk Function Perspective: COBIT 5 Enablers supporting Risk Governance and Management Activities

Processes

Organisational Structures

Culture, Ethics & Behaviour

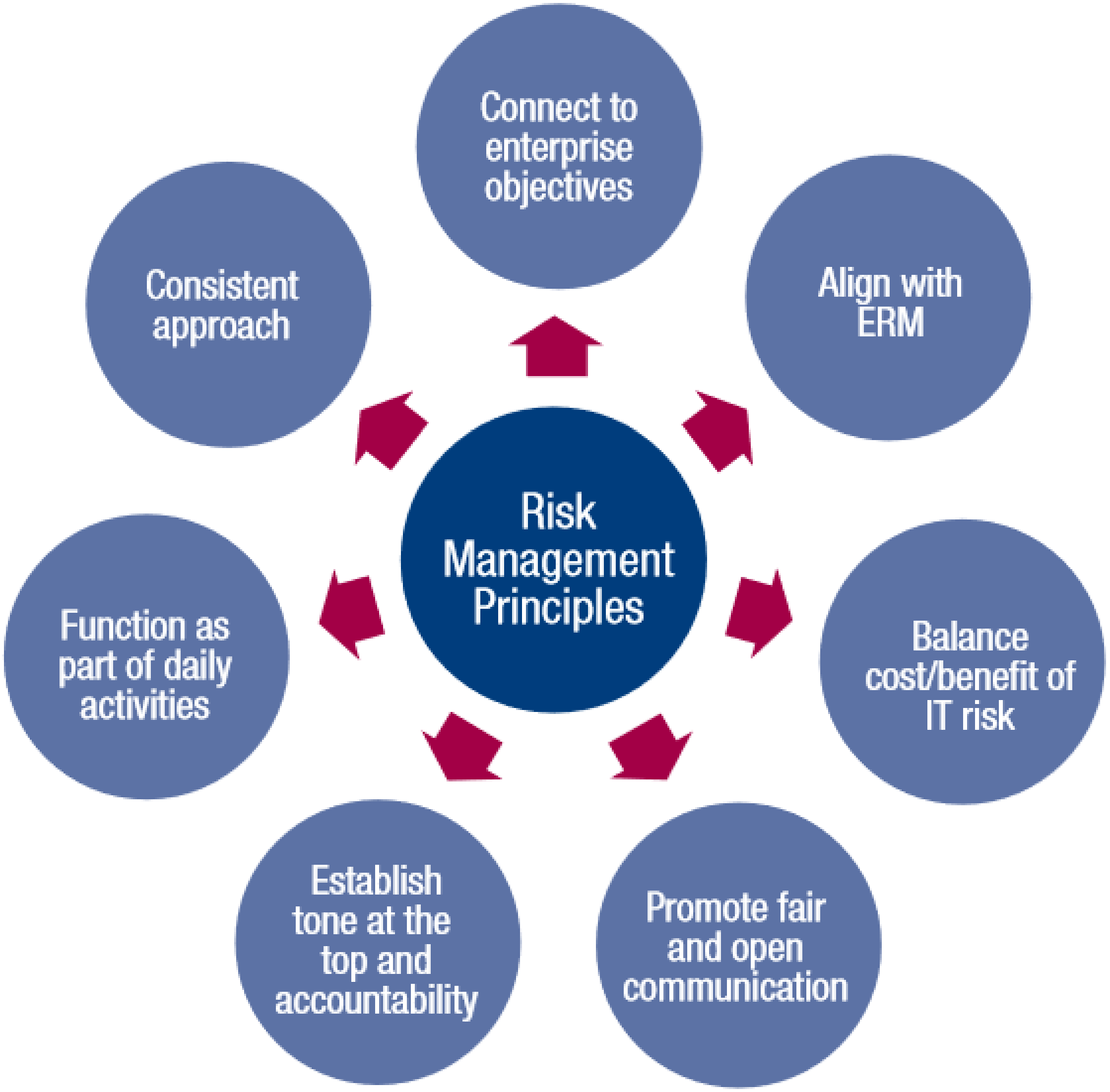
Principles, Policies & Frameworks

Information

Services, Infrastructure & Applications

People, Skills & Competences

## ENABLER RISK FUNCTION: PRINCIPLES, POLICIES & FRAMEWORKS



Risk Management Principles

Connect to enterprise objectives

Align with ERM

Balance cost/benefit of IT risk

Promote fair and open communication

Establish tone at the top and accountability

Function as part of daily activities

Consistent approach

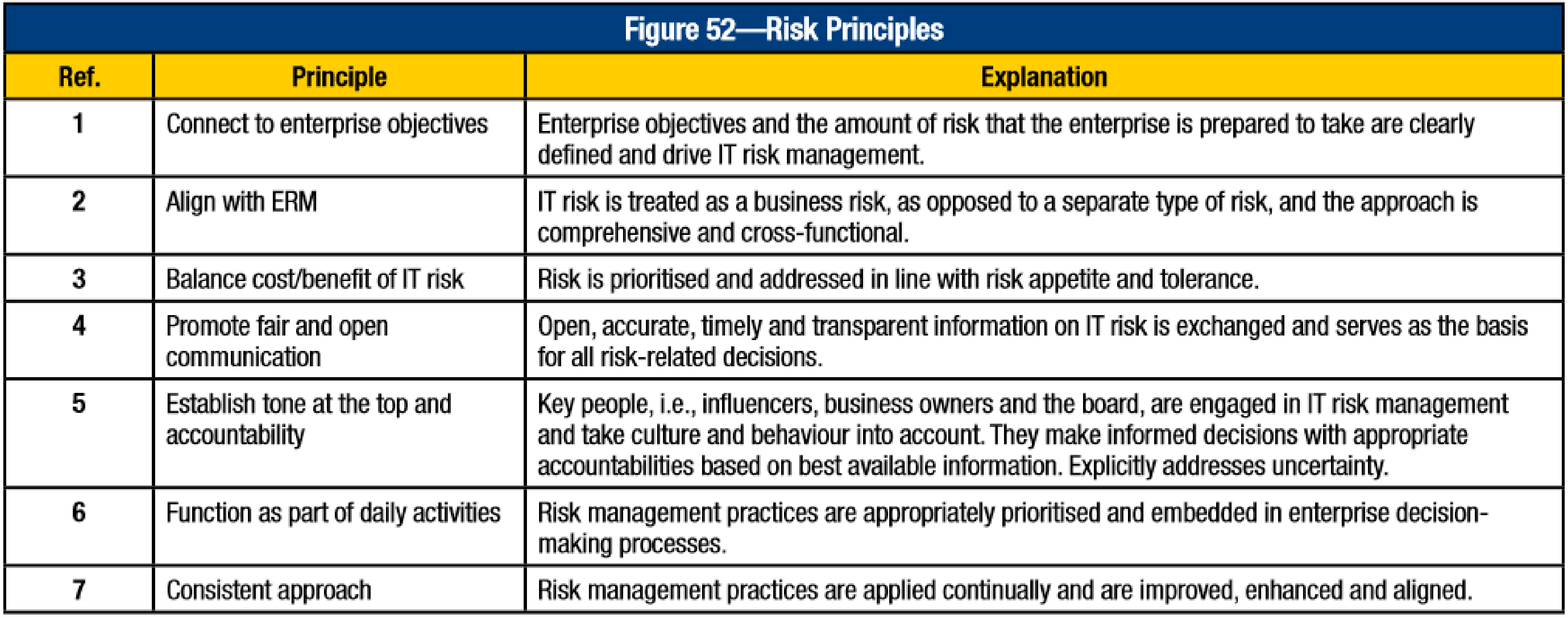
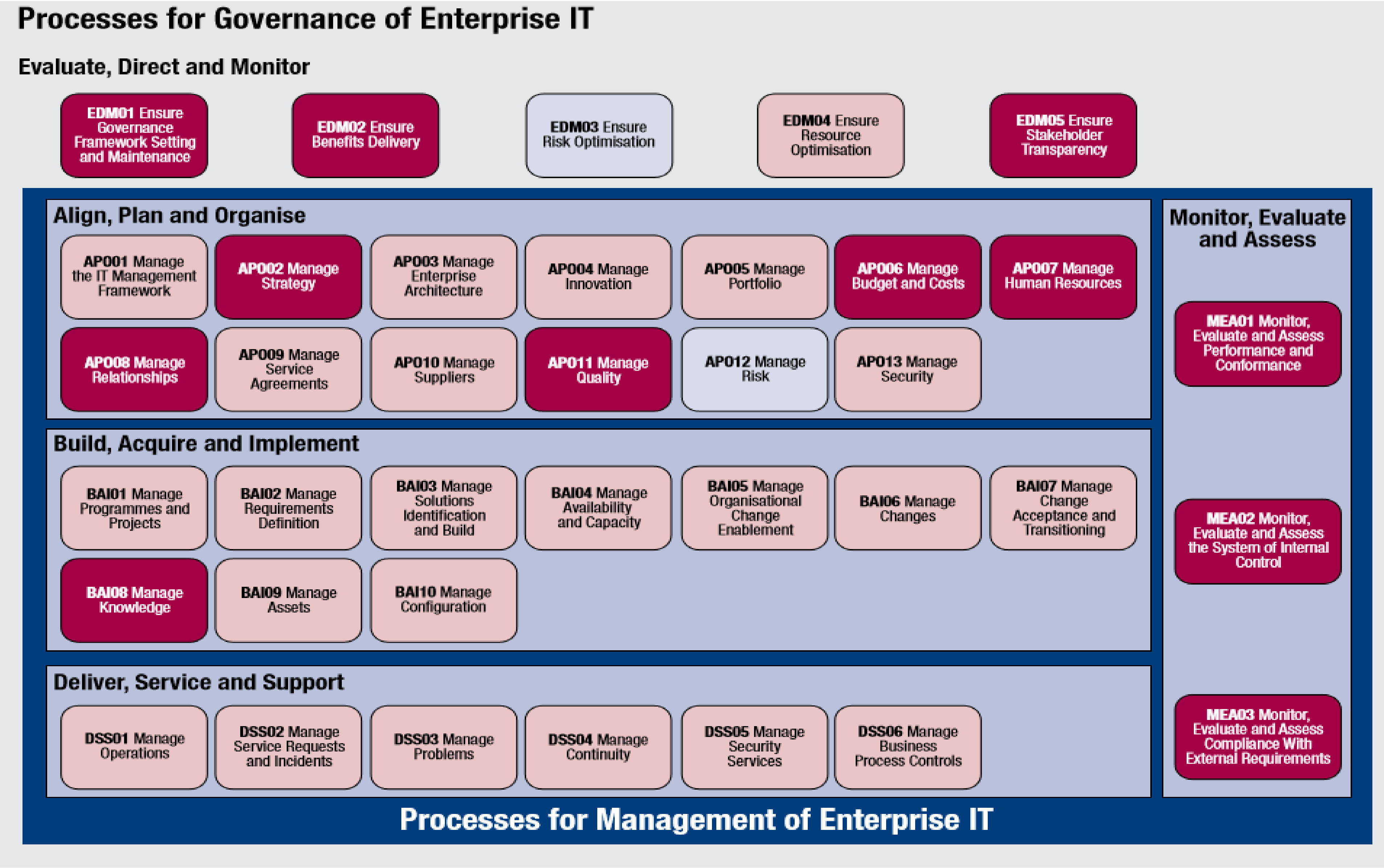


**Figure 52—Risk Principles**

| Ref. | Principle | Explanation |
|---|---|---|
| 1 | Connect to enterprise objectives | Enterprise objectives and the amount of risk that the enterprise is prepared to take are clearly defined and drive IT risk management. |
| 2 | Align with ERM | IT risk is treated as a business risk, as opposed to a separate type of risk, and the approach is comprehensive and cross-functional. |
| 3 | Balance cost/benefit of IT risk | Risk is prioritised and addressed in line with risk appetite and tolerance. |
| 4 | Promote fair and open communication | Open, accurate, timely and transparent information on IT risk is exchanged and serves as the basis for all risk-related decisions. |
| 5 | Establish tone at the top and accountability | Key people, i.e., influencers, business owners and the board, are engaged in IT risk management and take culture and behaviour into account. They make informed decisions with appropriate accountabilities based on best available information. Explicitly addresses uncertainty. |
| 6 | Function as part of daily activities | Risk management practices are appropriately prioritised and embedded in enterprise decision-making processes. |
| 7 | Consistent approach | Risk management practices are applied continually and are improved, enhanced and aligned. |

# ENABLER RISK FUNCTION: PROCESSES



## Processes for Governance of Enterprise IT

### Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

### Align, Plan and Organise

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

### Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

### Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

### Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

## Processes for Management of Enterprise IT

Figure 55—Risk Function Key Supporting Processes

| Process Identification | Justification | Output |
|---|---|---|
| EDM01 Ensure Governance Framework Setting and Maintenance | Governing and managing risk requires the setup of an adequate governance framework, to put in place enabling structures, principles, processes and practices. | Risk governance guiding principles |
| EDM02 Ensure Benefits Delivery | This process focuses on managing the value that the risk function generates. | Actions to improve risk value delivery |
| EDM05 Ensure Stakeholder Transparency | The enterprise risk function requires transparent performance and conformance measurement, with goals and metrics approved by stakeholders. | Evaluation of risk reporting requirements |
| APO02 Manage Strategy | IT risk management strategy must be well defined and aligned to ERM approach. | Risk management strategy |
| APO06 Manage Budget and Costs | The risk function needs to be budgeted. | Financial and budgetary requirements |
| APO07 Manage Human Resources | Risk management requires the right amount of people, skills and experience. | HR competencies framework |
| APO08 Manage Relationships | Maintain the relationships between the risk function and the business. | Communication plan |
| APO11 Manage Quality | Quality is an essential component of an effective risk management. | Quality review of risk deliverables |
| BAI08 Manage Knowledge | The risk function needs to be provided with the knowledge required to support staff in their work activities. | Classification of risk function information, access control over information, rules for disposal of information |
| MEA01 Monitor, Evaluate and Assess Performance and Conformance | Risk is a key aspect in the monitoring, evaluating and assessing of business and IT. | Risk monitoring metrics and targets |
| MEA02 Monitor, Evaluate and Assess the System of Internal Control | Internal controls are key in monitoring and containing risk, to avoid risk becoming an issue. | Results of internal control monitoring and reviews |
| MEA03 Monitor, Evaluate and Assess Compliance With External Requirements | Compliance with laws, regulations and contractual requirements represent risk and have to be monitored, evaluated and assessed in alignment with enterprise strategy. | Reports of non-compliance issues and root causes |

# ENABLER RISK FUNCTION: ORGANISATIONAL STRUCTURES

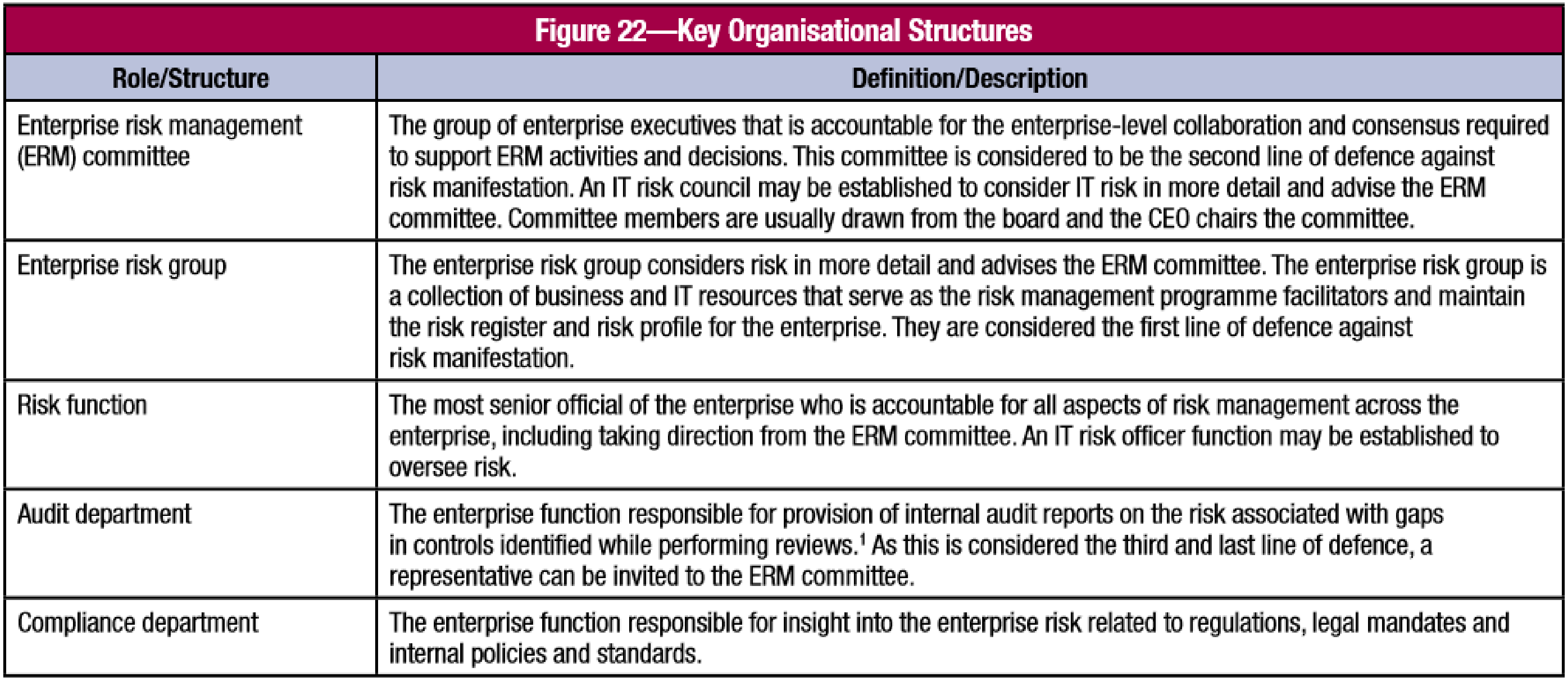
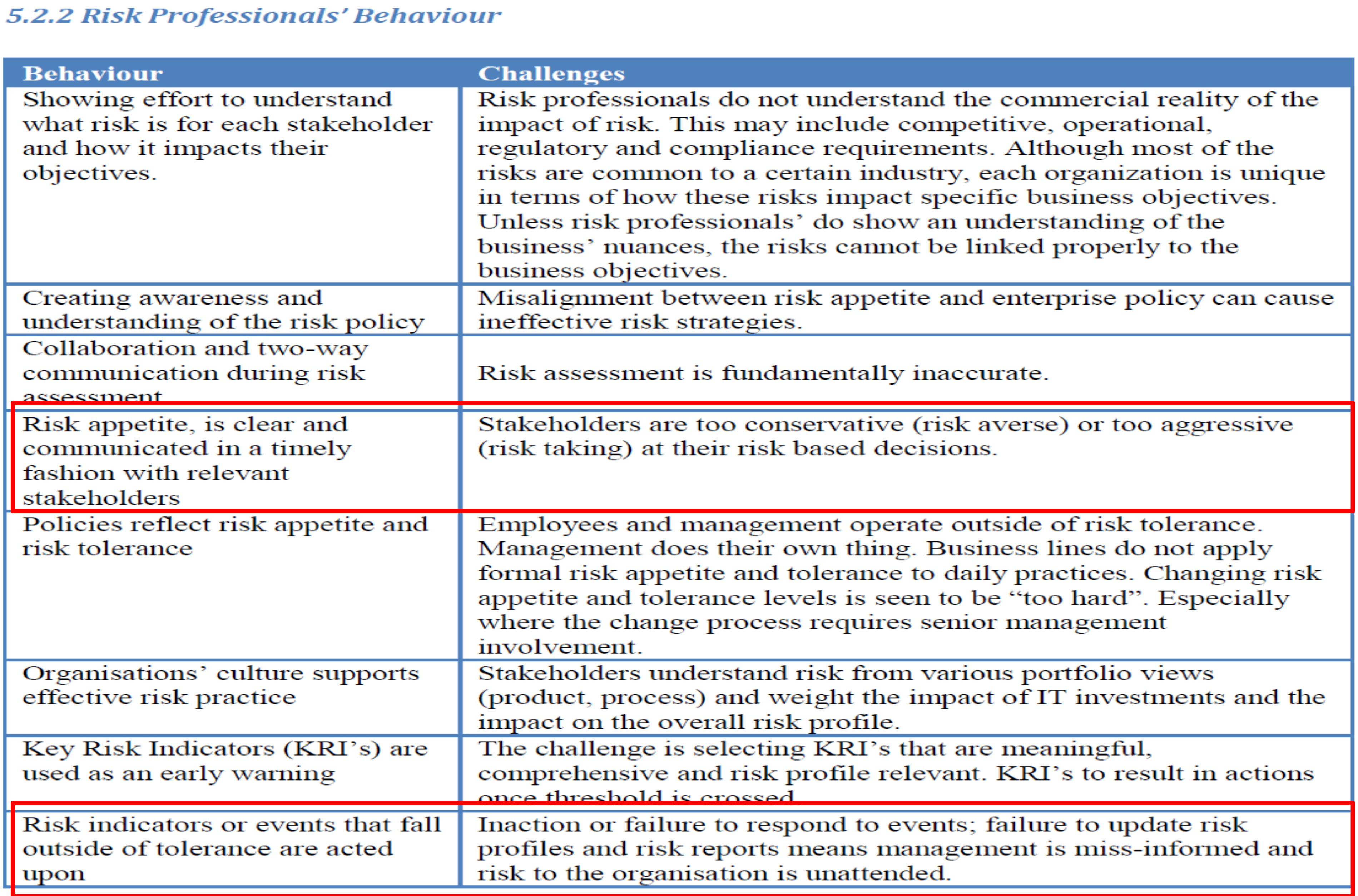


**Figure 22—Key Organisational Structures**

| Role/Structure | Definition/Description |
|---|---|
| Enterprise risk management (ERM) committee | The group of enterprise executives that is accountable for the enterprise-level collaboration and consensus required to support ERM activities and decisions. This committee is considered to be the second line of defence against risk manifestation. An IT risk council may be established to consider IT risk in more detail and advise the ERM committee. Committee members are usually drawn from the board and the CEO chairs the committee. |
| Enterprise risk group | The enterprise risk group considers risk in more detail and advises the ERM committee. The enterprise risk group is a collection of business and IT resources that serve as the risk management programme facilitators and maintain the risk register and risk profile for the enterprise. They are considered the first line of defence against risk manifestation. |
| Risk function | The most senior official of the enterprise who is accountable for all aspects of risk management across the enterprise, including taking direction from the ERM committee. An IT risk officer function may be established to oversee risk. |
| Audit department | The enterprise function responsible for provision of internal audit reports on the risk associated with gaps in controls identified while performing reviews.[1] As this is considered the third and last line of defence, a representative can be invited to the ERM committee. |
| Compliance department | The enterprise function responsible for insight into the enterprise risk related to regulations, legal mandates and internal policies and standards. |

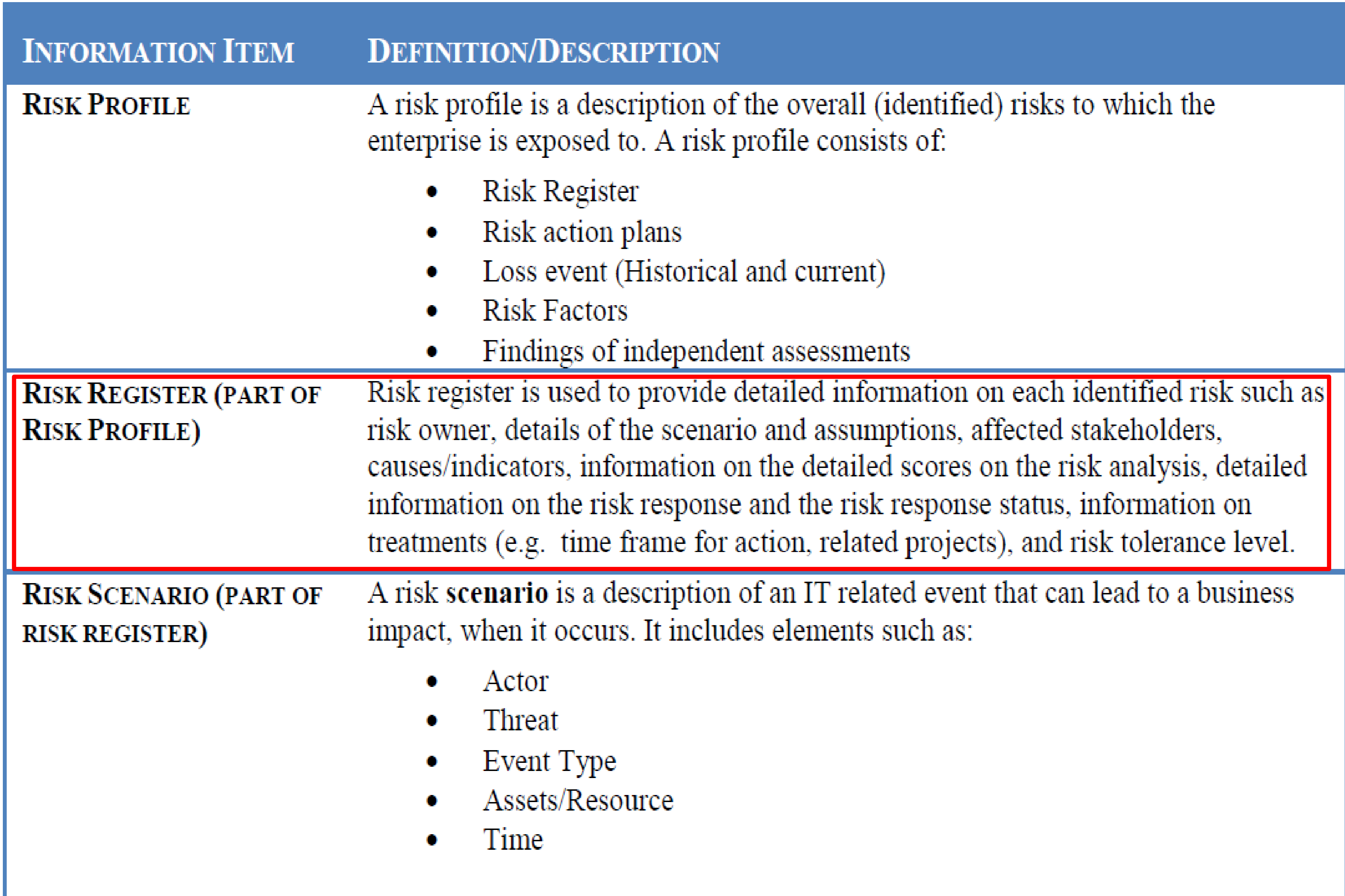
# ENABLER RISK FUNCTION: CULTURE, ETHICS & BEHAVIOUR



## 5.2.2 Risk Professionals' Behaviour

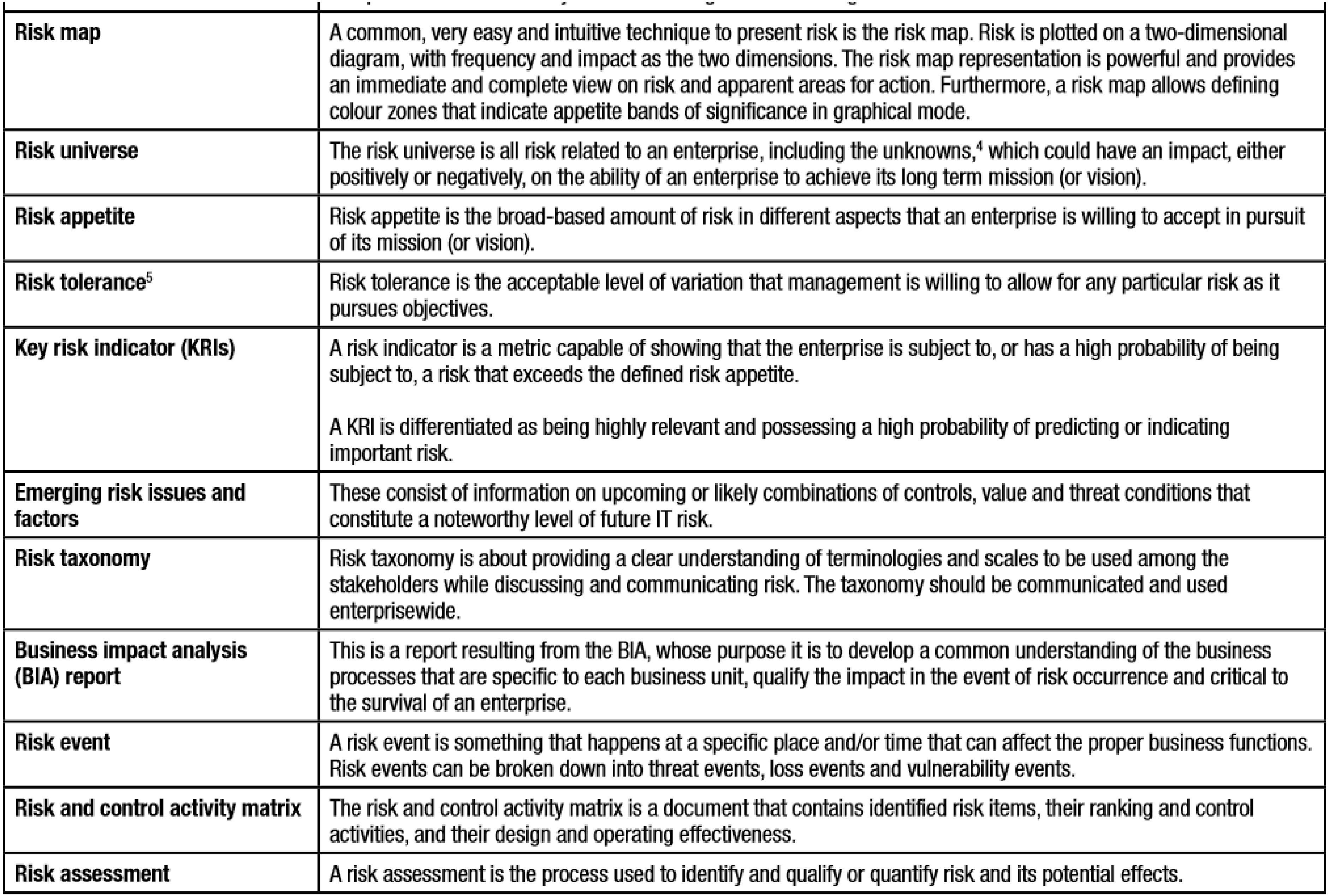
| Behaviour | Challenges |
|---|---|
| Showing effort to understand what risk is for each stakeholder and how it impacts their objectives. | Risk professionals do not understand the commercial reality of the impact of risk. This may include competitive, operational, regulatory and compliance requirements. Although most of the risks are common to a certain industry, each organization is unique in terms of how these risks impact specific business objectives. Unless risk professionals' do show an understanding of the business' nuances, the risks cannot be linked properly to the business objectives. |
| Creating awareness and understanding of the risk policy | Misalignment between risk appetite and enterprise policy can cause ineffective risk strategies. |
| Collaboration and two-way communication during risk assessment | Risk assessment is fundamentally inaccurate. |
| Risk appetite, is clear and communicated in a timely fashion with relevant stakeholders | Stakeholders are too conservative (risk averse) or too aggressive (risk taking) at their risk based decisions. |
| Policies reflect risk appetite and risk tolerance | Employees and management operate outside of risk tolerance. Management does their own thing. Business lines do not apply formal risk appetite and tolerance to daily practices. Changing risk appetite and tolerance levels is seen to be "too hard". Especially where the change process requires senior management involvement. |
| Organisations' culture supports effective risk practice | Stakeholders understand risk from various portfolio views (product, process) and weight the impact of IT investments and the impact on the overall risk profile. |
| Key Risk Indicators (KRI's) are used as an early warning | The challenge is selecting KRI's that are meaningful, comprehensive and risk profile relevant. KRI's to result in actions once threshold is crossed. |
| Risk indicators or events that fall outside of tolerance are acted upon | Inaction or failure to respond to events; failure to update risk profiles and risk reports means management is miss-informed and risk to the organisation is unattended. |

# ENABLER RISK FUNCTION: INFORMATION



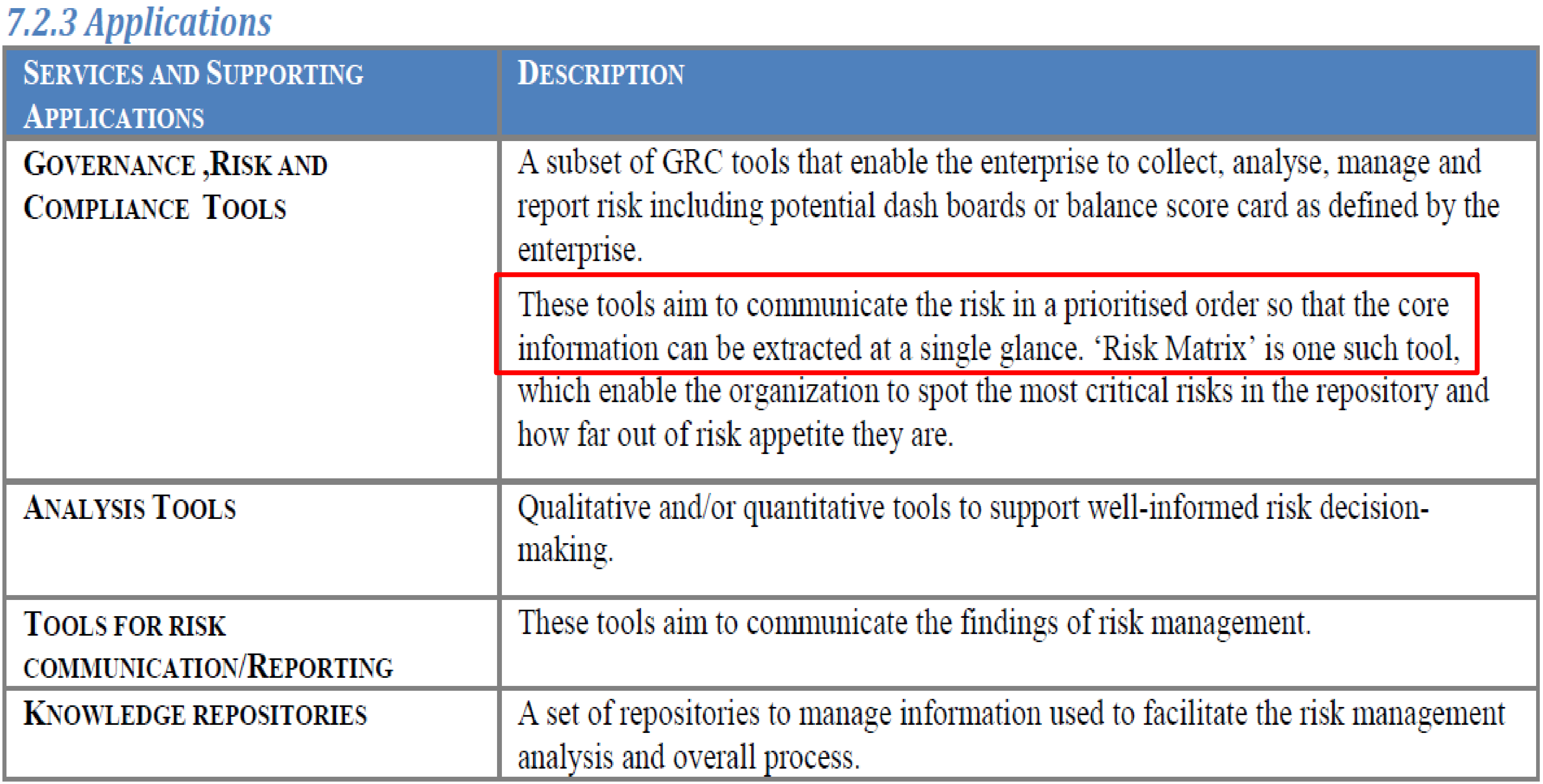
| INFORMATION ITEM | DEFINITION/DESCRIPTION |
|---|---|
| RISK PROFILE | A risk profile is a description of the overall (identified) risks to which the enterprise is exposed to. A risk profile consists of:<br>• Risk Register<br>• Risk action plans<br>• Loss event (Historical and current)<br>• Risk Factors<br>• Findings of independent assessments |
| RISK REGISTER (PART OF RISK PROFILE) | Risk register is used to provide detailed information on each identified risk such as risk owner, details of the scenario and assumptions, affected stakeholders, causes/indicators, information on the detailed scores on the risk analysis, detailed information on the risk response and the risk response status, information on treatments (e.g. time frame for action, related projects), and risk tolerance level. |
| RISK SCENARIO (PART OF RISK REGISTER) | A risk **scenario** is a description of an IT related event that can lead to a business impact, when it occurs. It includes elements such as:<br>• Actor<br>• Threat<br>• Event Type<br>• Assets/Resource<br>• Time |

# ENABLER RISK FUNCTION: INFORMATION



| | |
|---|---|
| **Risk map** | A common, very easy and intuitive technique to present risk is the risk map. Risk is plotted on a two-dimensional diagram, with frequency and impact as the two dimensions. The risk map representation is powerful and provides an immediate and complete view on risk and apparent areas for action. Furthermore, a risk map allows defining colour zones that indicate appetite bands of significance in graphical mode. |
| **Risk universe** | The risk universe is all risk related to an enterprise, including the unknowns,[4] which could have an impact, either positively or negatively, on the ability of an enterprise to achieve its long term mission (or vision). |
| **Risk appetite** | Risk appetite is the broad-based amount of risk in different aspects that an enterprise is willing to accept in pursuit of its mission (or vision). |
| **Risk tolerance**[5] | Risk tolerance is the acceptable level of variation that management is willing to allow for any particular risk as it pursues objectives. |
| **Key risk indicator (KRIs)** | A risk indicator is a metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite.<br>A KRI is differentiated as being highly relevant and possessing a high probability of predicting or indicating important risk. |
| **Emerging risk issues and factors** | These consist of information on upcoming or likely combinations of controls, value and threat conditions that constitute a noteworthy level of future IT risk. |
| **Risk taxonomy** | Risk taxonomy is about providing a clear understanding of terminologies and scales to be used among the stakeholders while discussing and communicating risk. The taxonomy should be communicated and used enterprisewide. |
| **Business impact analysis (BIA) report** | This is a report resulting from the BIA, whose purpose it is to develop a common understanding of the business processes that are specific to each business unit, qualify the impact in the event of risk occurrence and critical to the survival of an enterprise. |
| **Risk event** | A risk event is something that happens at a specific place and/or time that can affect the proper business functions. Risk events can be broken down into threat events, loss events and vulnerability events. |
| **Risk and control activity matrix** | The risk and control activity matrix is a document that contains identified risk items, their ranking and control activities, and their design and operating effectiveness. |
| **Risk assessment** | A risk assessment is the process used to identify and qualify or quantify risk and its potential effects. |

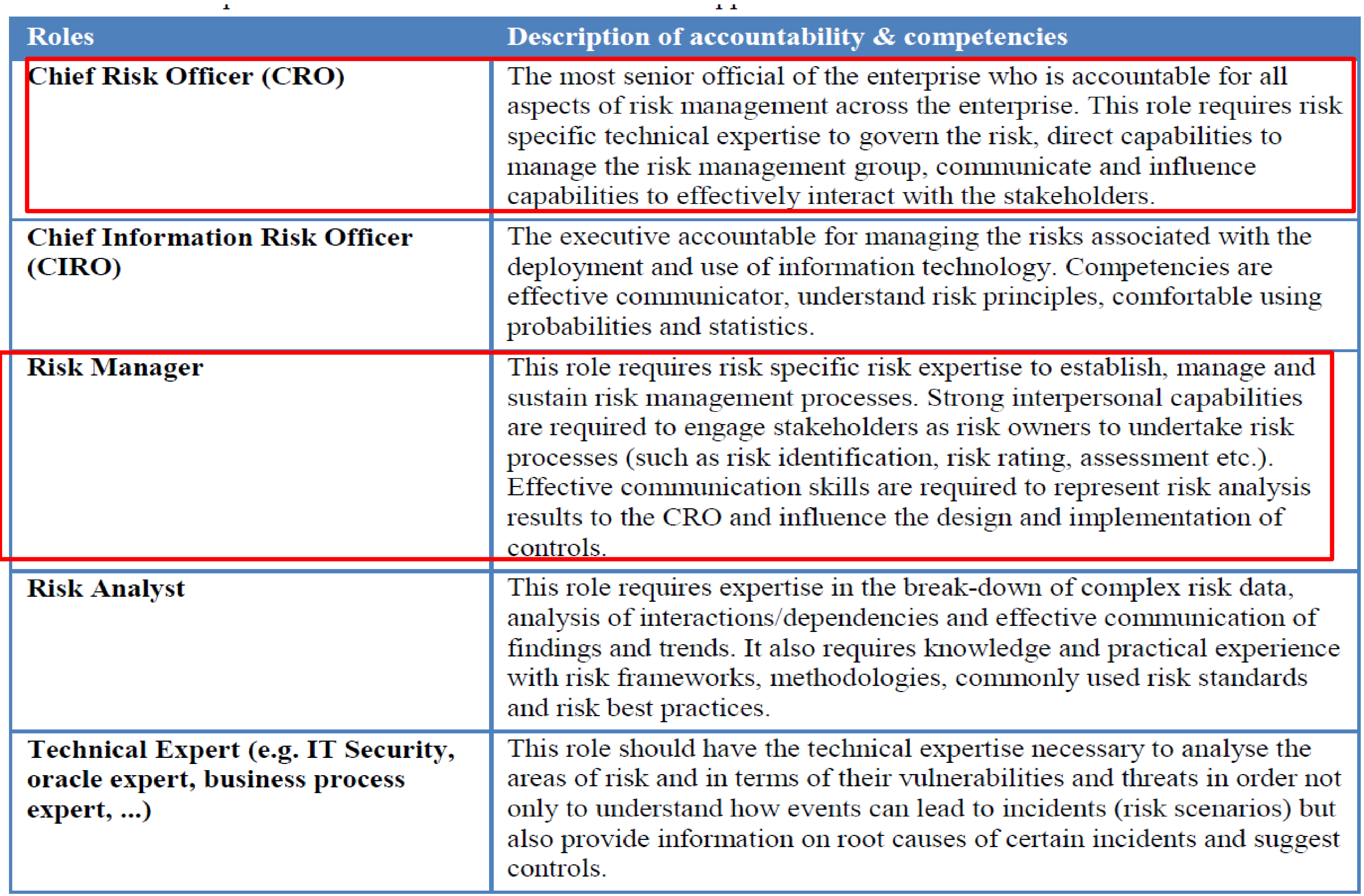
# ENABLER RISK FUNCTION: SERVICES, INFRASTRUCTURES & APPLICATIONS



## 7.2.3 Applications

| Services and Supporting Applications | Description |
|---|---|
| Governance ,Risk and Compliance Tools | A subset of GRC tools that enable the enterprise to collect, analyse, manage and report risk including potential dash boards or balance score card as defined by the enterprise.<br>These tools aim to communicate the risk in a prioritised order so that the core information can be extracted at a single glance. 'Risk Matrix' is one such tool, which enable the organization to spot the most critical risks in the repository and how far out of risk appetite they are. |
| Analysis Tools | Qualitative and/or quantitative tools to support well-informed risk decision-making. |
| Tools for risk communication/Reporting | These tools aim to communicate the findings of risk management. |
| Knowledge repositories | A set of repositories to manage information used to facilitate the risk management analysis and overall process. |

## ENABLER RISK FUNCTION: PEOPLE, SKILLS & COMPETENCIES



| Roles | Description of accountability & competencies |
|---|---|
| **Chief Risk Officer (CRO)** | The most senior official of the enterprise who is accountable for all aspects of risk management across the enterprise. This role requires risk specific technical expertise to govern the risk, direct capabilities to manage the risk management group, communicate and influence capabilities to effectively interact with the stakeholders. |
| **Chief Information Risk Officer (CIRO)** | The executive accountable for managing the risks associated with the deployment and use of information technology. Competencies are effective communicator, understand risk principles, comfortable using probabilities and statistics. |
| **Risk Manager** | This role requires risk specific risk expertise to establish, manage and sustain risk management processes. Strong interpersonal capabilities are required to engage stakeholders as risk owners to undertake risk processes (such as risk identification, risk rating, assessment etc.). Effective communication skills are required to represent risk analysis results to the CRO and influence the design and implementation of controls. |
| **Risk Analyst** | This role requires expertise in the break-down of complex risk data, analysis of interactions/dependencies and effective communication of findings and trends. It also requires knowledge and practical experience with risk frameworks, methodologies, commonly used risk standards and risk best practices. |
| **Technical Expert (e.g. IT Security, oracle expert, business process expert, ...)** | This role should have the technical expertise necessary to analyse the areas of risk and in terms of their vulnerabilities and threats in order not only to understand how events can lead to incidents (risk scenarios) but also provide information on root causes of certain incidents and suggest controls. |

# ENABLER RISK FUNCTION: PEOPLE, SKILLS & COMPETENCIES

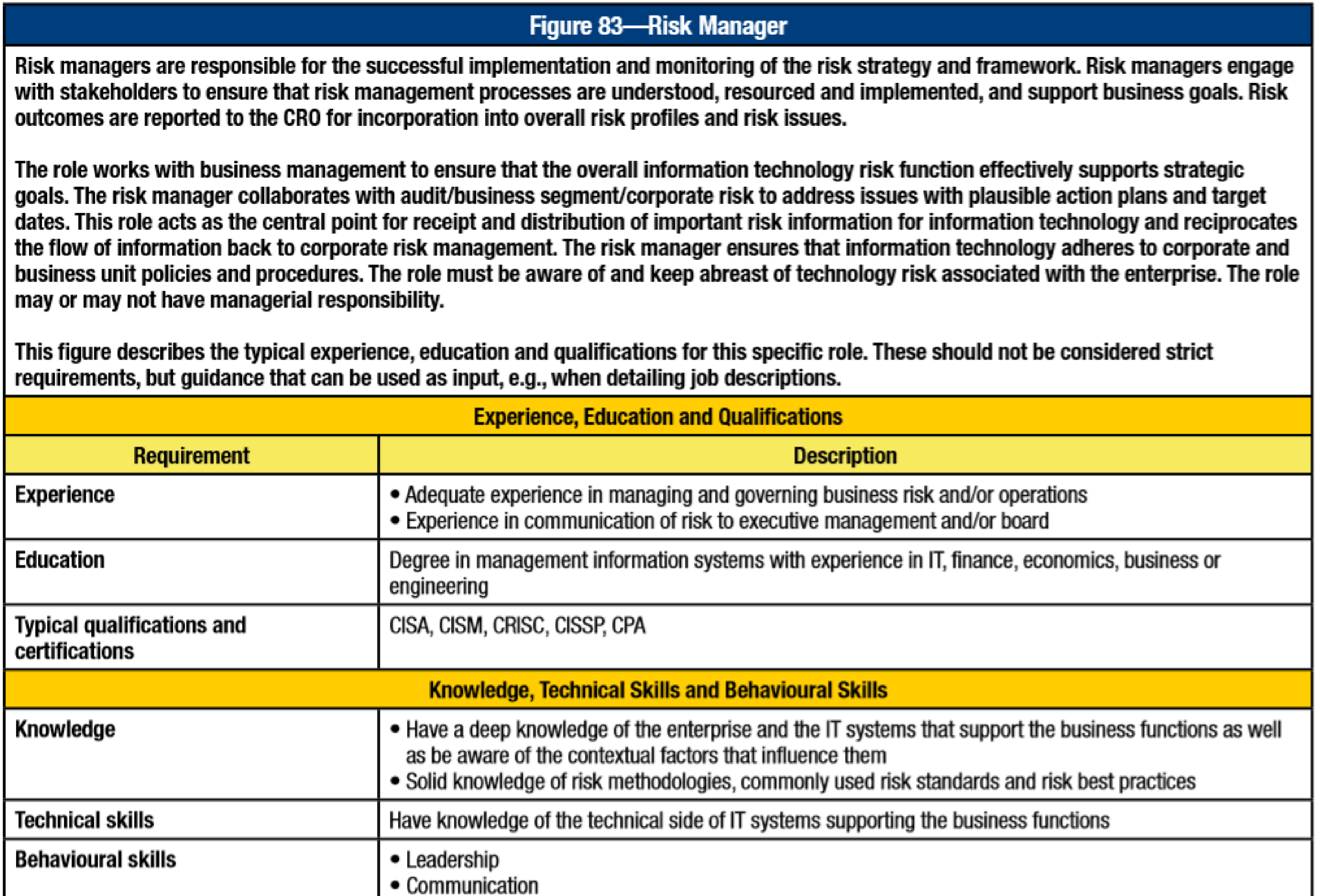


Figure 83—Risk Manager

Risk managers are responsible for the successful implementation and monitoring of the risk strategy and framework. Risk managers engage with stakeholders to ensure that risk management processes are understood, resourced and implemented, and support business goals. Risk outcomes are reported to the CRO for incorporation into overall risk profiles and risk issues.

The role works with business management to ensure that the overall information technology risk function effectively supports strategic goals. The risk manager collaborates with audit/business segment/corporate risk to address issues with plausible action plans and target dates. This role acts as the central point for receipt and distribution of important risk information for information technology and reciprocates the flow of information back to corporate risk management. The risk manager ensures that information technology adheres to corporate and business unit policies and procedures. The role must be aware of and keep abreast of technology risk associated with the enterprise. The role may or may not have managerial responsibility.

This figure describes the typical experience, education and qualifications for this specific role. These should not be considered strict requirements, but guidance that can be used as input, e.g., when detailing job descriptions.

| Requirement | Description |
|---|---|
| **Experience, Education and Qualifications** | |
| Experience | • Adequate experience in managing and governing business risk and/or operations<br>• Experience in communication of risk to executive management and/or board |
| Education | Degree in management information systems with experience in IT, finance, economics, business or engineering |
| Typical qualifications and certifications | CISA, CISM, CRISC, CISSP, CPA |
| **Knowledge, Technical Skills and Behavioural Skills** | |
| Knowledge | • Have a deep knowledge of the enterprise and the IT systems that support the business functions as well as be aware of the contextual factors that influence them<br>• Solid knowledge of risk methodologies, commonly used risk standards and risk best practices |
| Technical skills | Have knowledge of the technical side of IT systems supporting the business functions |
| Behavioural skills | • Leadership<br>• Communication |

# ENABLER RISK FUNCTION: PEOPLE, SKILLS & COMPETENCIES

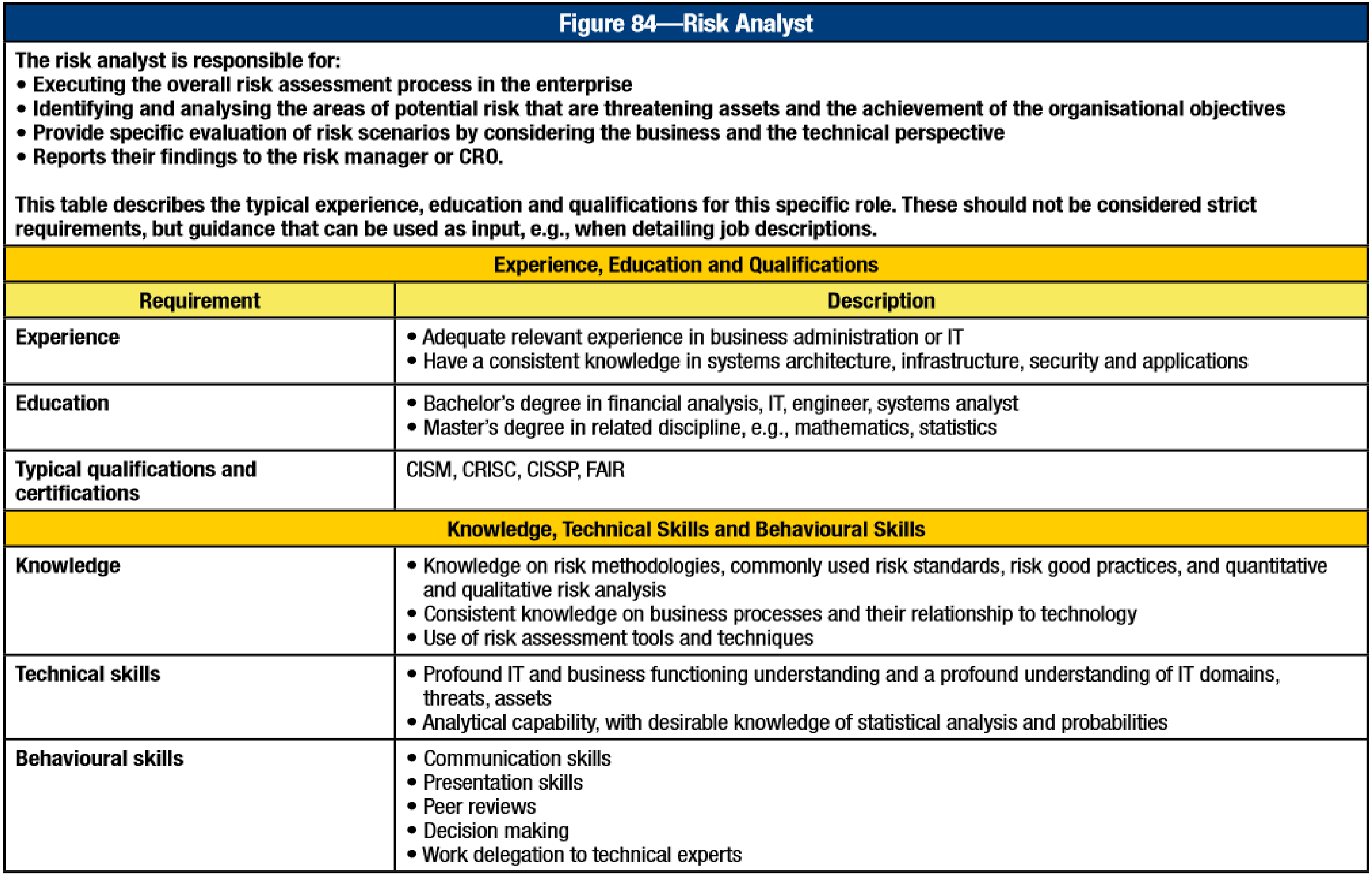


**Figure 84—Risk Analyst**

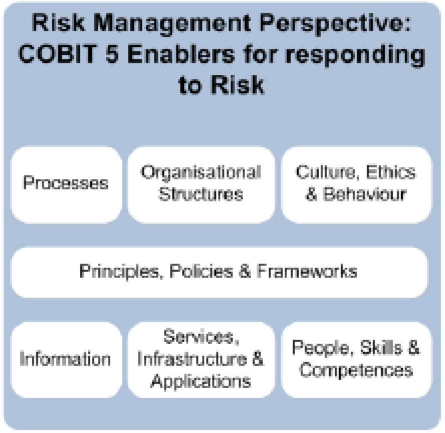
**The risk analyst is responsible for:**

- **Executing the overall risk assessment process in the enterprise**
- **Identifying and analysing the areas of potential risk that are threatening assets and the achievement of the organisational objectives**
- **Provide specific evaluation of risk scenarios by considering the business and the technical perspective**
- **Reports their findings to the risk manager or CRO.**

**This table describes the typical experience, education and qualifications for this specific role. These should not be considered strict requirements, but guidance that can be used as input, e.g., when detailing job descriptions.**

| | |
|---|---|
| **Experience, Education and Qualifications** | |
| **Requirement** | **Description** |
| **Experience** | • Adequate relevant experience in business administration or IT<br>• Have a consistent knowledge in systems architecture, infrastructure, security and applications |
| **Education** | • Bachelor's degree in financial analysis, IT, engineer, systems analyst<br>• Master's degree in related discipline, e.g., mathematics, statistics |
| **Typical qualifications and certifications** | CISM, CRISC, CISSP, FAIR |
| **Knowledge, Technical Skills and Behavioural Skills** | |
| **Knowledge** | • Knowledge on risk methodologies, commonly used risk standards, risk good practices, and quantitative and qualitative risk analysis<br>• Consistent knowledge on business processes and their relationship to technology<br>• Use of risk assessment tools and techniques |
| **Technical skills** | • Profound IT and business functioning understanding and a profound understanding of IT domains, threats, assets<br>• Analytical capability, with desirable knowledge of statistical analysis and probabilities |
| **Behavioural skills** | • Communication skills<br>• Presentation skills<br>• Peer reviews<br>• Decision making<br>• Work delegation to technical experts |

# RISK MANAGEMENT PERSPECTIVE



**Risk Management Perspective: COBIT 5 Enablers for responding to Risk**

Processes

Organisational Structures

Culture, Ethics & Behaviour

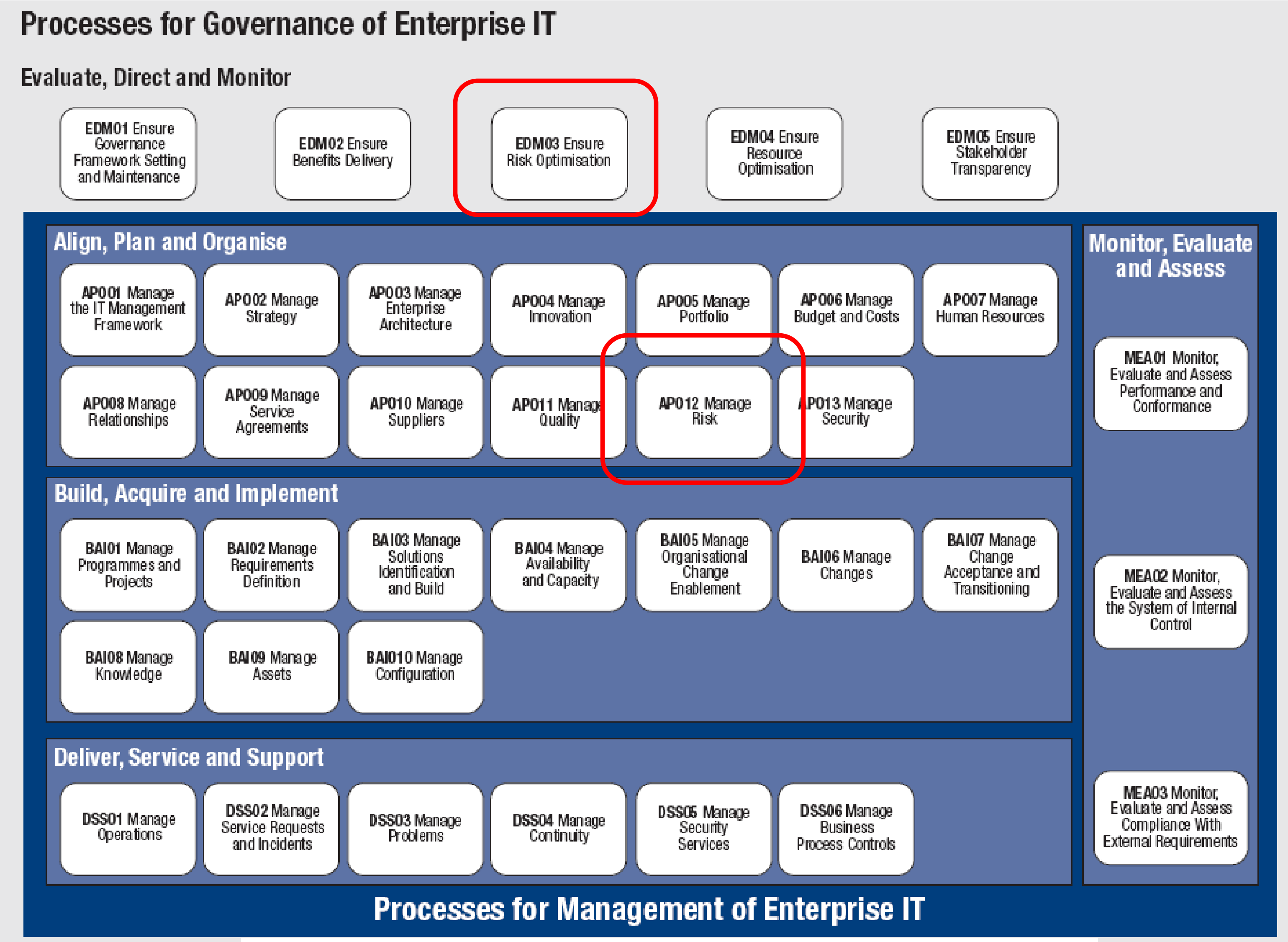
Principles, Policies & Frameworks

Information

Services, Infrastructure & Applications

People, Skills & Competences

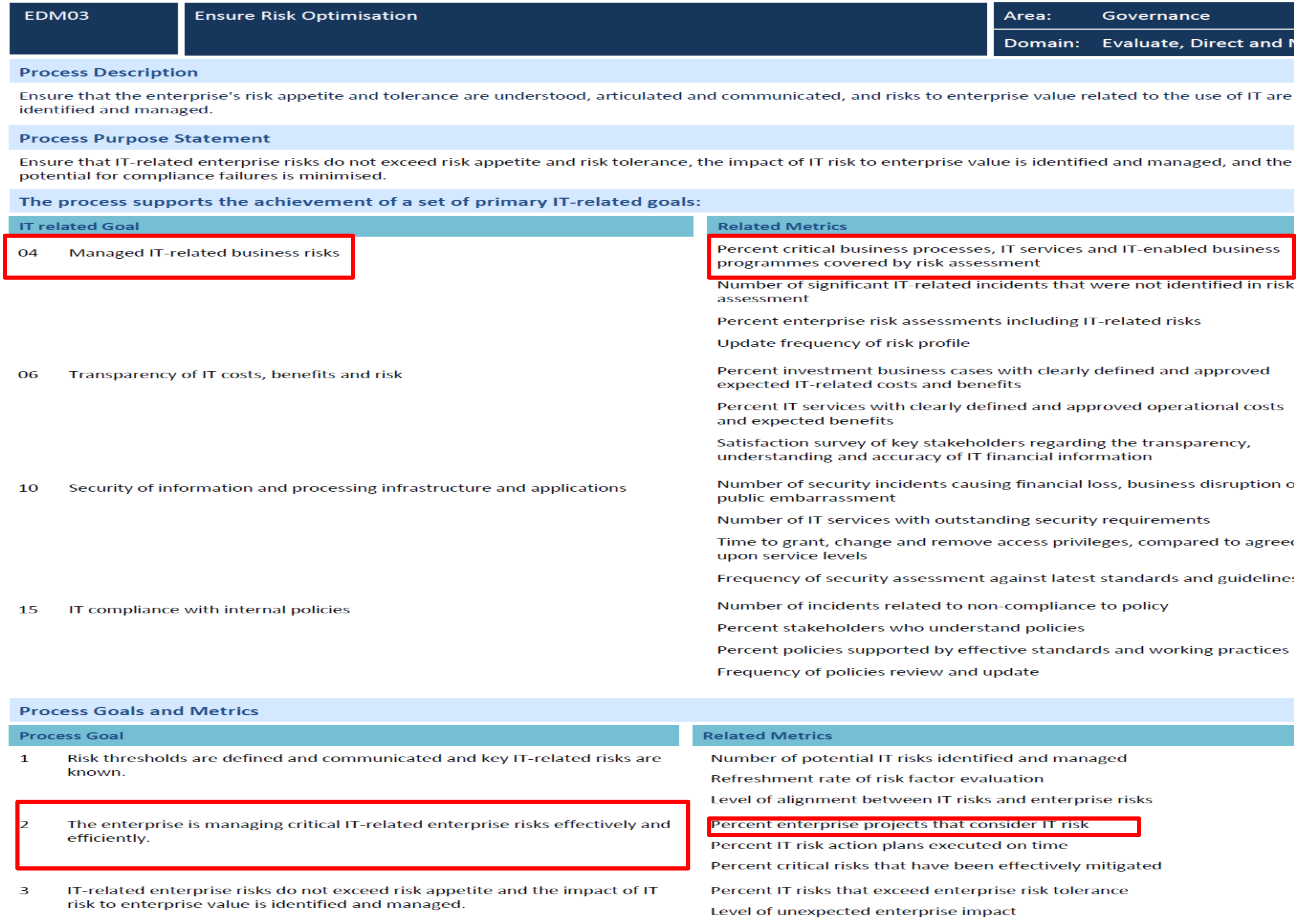
# Risk Management in COBIT 5


Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
APO01 Manage the IT Management Framework
APO02 Manage Strategy
APO03 Manage Enterprise Architecture
APO04 Manage Innovation
APO05 Manage Portfolio
APO06 Manage Budget and Costs
APO07 Manage Human Resources
APO08 Manage Relationships
APO09 Manage Service Agreements
APO10 Manage Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI010 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Processes for Management of Enterprise IT

Source: COBIT® 5, figure 16. © 2012 ISACA® All rights reserved.

## RISK GOVERNANCE & MANAGEMENT PROCESS

- All enterprise activities have associated risk exposures resulting from environmental threats that exploit enabler vulnerabilities
  - **EDM03 Ensure risk optimisation** ensures that the enterprise stakeholders approach to risk is articulated to direct how risks facing the enterprise will be treated.
  - **APO12 Manage risk** provides the enterprise risk management (ERM) arrangements that ensure that the stakeholder direction is followed by the enterprise.
  - **All other processes** include practices and activities that are designed to treat related risk (avoid, reduce/mitigate/control, share/transfer/accept).



| EDM03 | Ensure Risk Optimisation | Area: | Governance |
|---|---|---|---|
| | | Domain: | Evaluate, Direct and M |

## Process Description

Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and risks to enterprise value related to the use of IT are identified and managed.

## Process Purpose Statement

Ensure that IT-related enterprise risks do not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.

## The process supports the achievement of a set of primary IT-related goals:

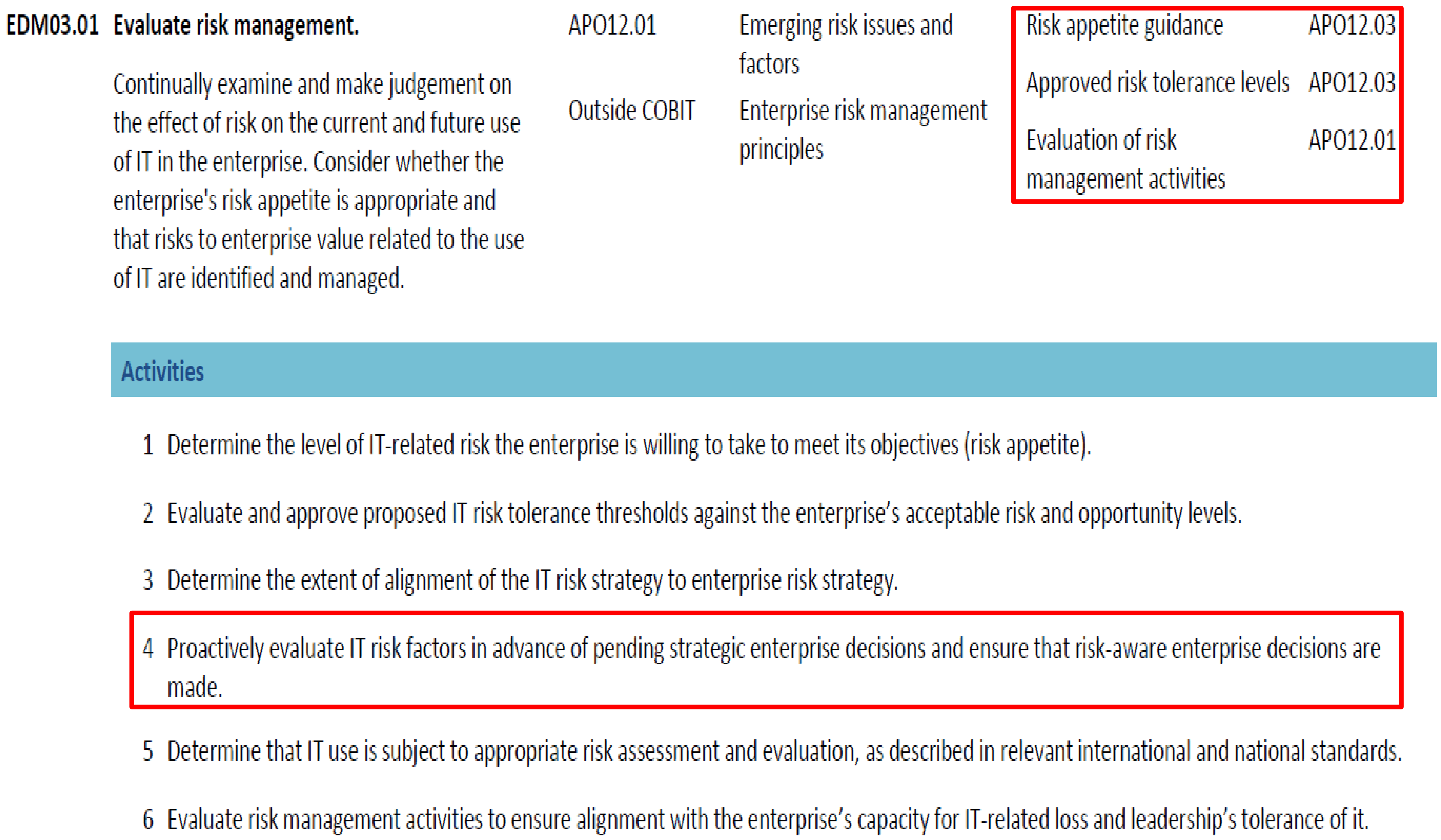
| IT related Goal | | Related Metrics |
|---|---|---|
| 04 | Managed IT-related business risks | Percent critical business processes, IT services and IT-enabled business programmes covered by risk assessment<br>Number of significant IT-related incidents that were not identified in risk assessment<br>Percent enterprise risk assessments including IT-related risks<br>Update frequency of risk profile |
| 06 | Transparency of IT costs, benefits and risk | Percent investment business cases with clearly defined and approved expected IT-related costs and benefits<br>Percent IT services with clearly defined and approved operational costs and expected benefits<br>Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information |
| 10 | Security of information and processing infrastructure and applications | Number of security incidents causing financial loss, business disruption o public embarrassment<br>Number of IT services with outstanding security requirements<br>Time to grant, change and remove access privileges, compared to agreed upon service levels<br>Frequency of security assessment against latest standards and guidelines |
| 15 | IT compliance with internal policies | Number of incidents related to non-compliance to policy<br>Percent stakeholders who understand policies<br>Percent policies supported by effective standards and working practices<br>Frequency of policies review and update |

## Process Goals and Metrics

| Process Goal | | Related Metrics |
|---|---|---|
| 1 | Risk thresholds are defined and communicated and key IT-related risks are known. | Number of potential IT risks identified and managed<br>Refreshment rate of risk factor evaluation<br>Level of alignment between IT risks and enterprise risks |
| 2 | The enterprise is managing critical IT-related enterprise risks effectively and efficiently. | Percent enterprise projects that consider IT risk<br>Percent IT risk action plans executed on time<br>Percent critical risks that have been effectively mitigated |
| 3 | IT-related enterprise risks do not exceed risk appetite and the impact of IT risk to enterprise value is identified and managed. | Percent IT risks that exceed enterprise risk tolerance<br>Level of unexpected enterprise impact |

## RACI Chart

| Key Governance Practice | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Project Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| EDM03.01 Evaluate risk management. | A | R | C | C | R | C | R |  |  | I | R | C |  | I | C | C | C | R | C |  |  |  |  |  |  | C |
| EDM03.02 Direct risk management. | A | R | C | C | R | C | R | I | I | I | R | I | I | I | C | C | C | R | C | I | I | I | I | I | I | I |
| EDM03.03 Monitor IT risk management. | A | R | C | C | R | C | R | I | I | I | R | R | I | I | C | C | C | R | C | I | I | I | I | I | I | C |



| | | | | |
|---|---|---|---|---|
| **EDM03.01 Evaluate risk management.**<br>Continually examine and make judgement on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed. | APO12.01 | Emerging risk issues and factors | Risk appetite guidance | APO12.03 |
| | Outside COBIT | Enterprise risk management principles | Approved risk tolerance levels | APO12.03 |
| | | | Evaluation of risk management activities | APO12.01 |

**Activities**

1 Determine the level of IT-related risk the enterprise is willing to take to meet its objectives (risk appetite).

2 Evaluate and approve proposed IT risk tolerance thresholds against the enterprise's acceptable risk and opportunity levels.

3 Determine the extent of alignment of the IT risk strategy to enterprise risk strategy.

4 Proactively evaluate IT risk factors in advance of pending strategic enterprise decisions and ensure that risk-aware enterprise decisions are made.

5 Determine that IT use is subject to appropriate risk assessment and evaluation, as described in relevant international and national standards.

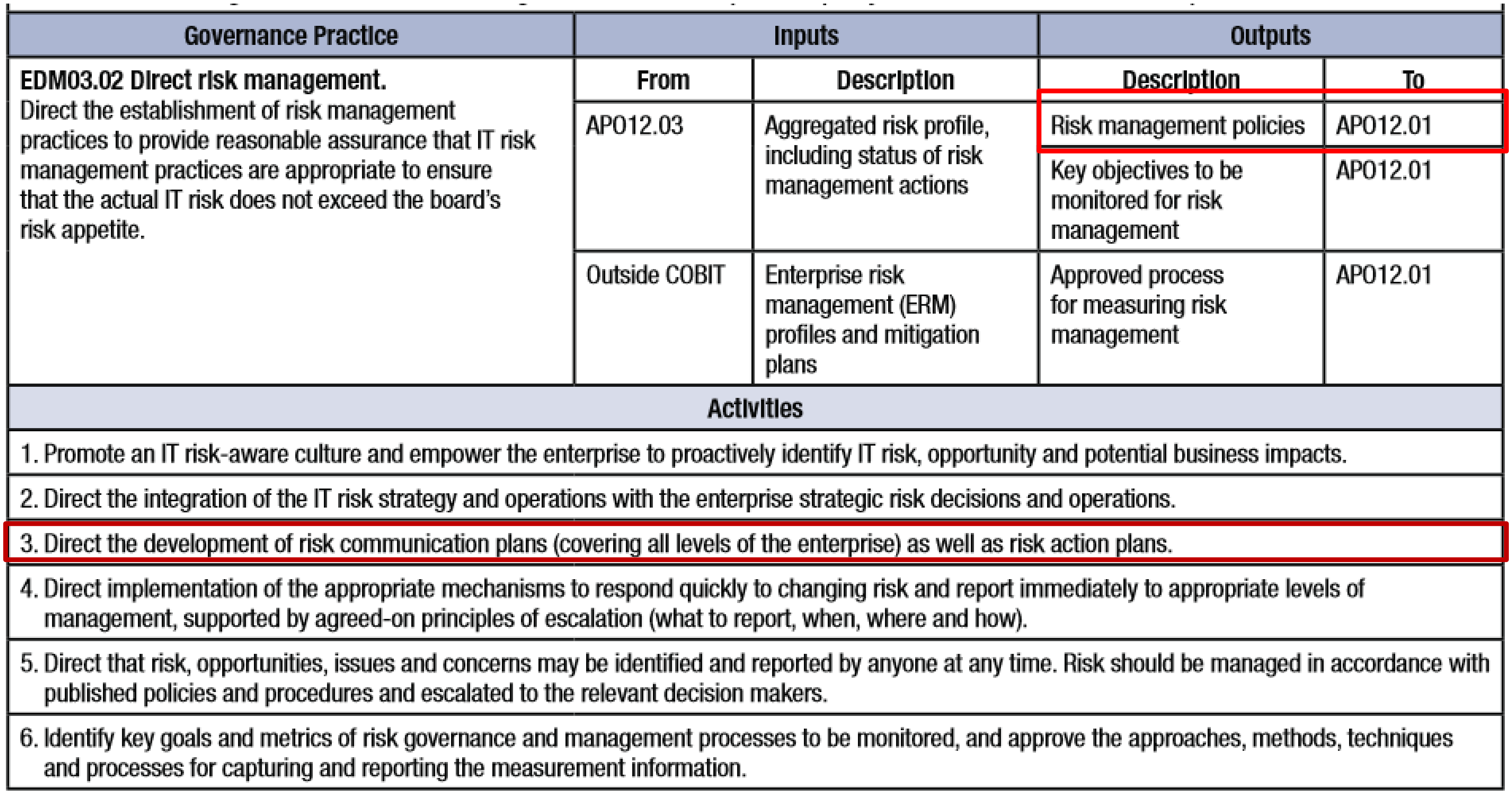
6 Evaluate risk management activities to ensure alignment with the enterprise's capacity for IT-related loss and leadership's tolerance of it.

**EDM03 Risk-specific Process Practices, Inputs/Outputs and Activities**

| Governance Practice | Risk-specific Inputs (in Addition to COBIT 5 Inputs) | | Risk-specific Outputs (in Addition to COBIT 5 Outputs) | |
|---|---|---|---|---|
| | From | Description | Description | To |
| **EDM03.1 Evaluate risk management.** Continually examine and make judgement on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risk to enterprise value related to the use of IT is identified and managed. | Risk-specific inputs and outputs are not relevant for this practice. The generic COBIT 5 inputs and outputs can be used as further guidance. | | | |

**Risk-specific Activities (in Addition to COBIT 5 Activities)**

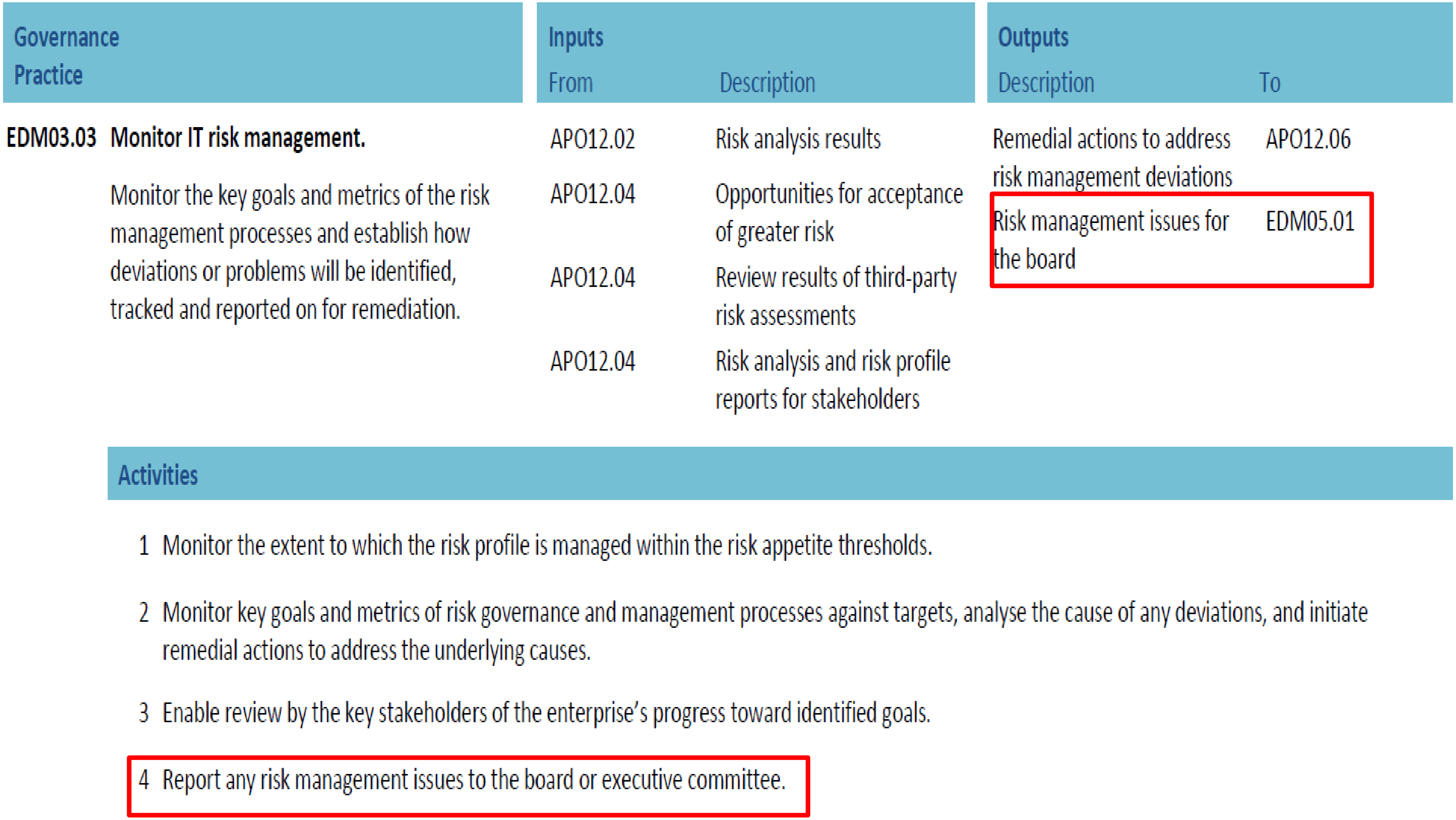
1. Determine the level of IT-related risk the enterprise is willing to take to meet its objectives (risk appetite).
   1.1 Perform enterprise IT risk assessment.
   1.2 Sponsor workshops with business management to discuss the broad amount of risk that the enterprise is willing to accept in pursuit of its objectives (risk appetite).
   1.3 Help business managers understand IT risk in the context of scenarios that affect their business and the objectives that matter most in their daily lives.
   1.4 Take a top-down, end-to-end look at business services and processes and identify the major points of IT support. Identify where value is generated and needs to be protected and sustained.
   1.5 Identify IT-related events and conditions that may jeopardise value, affect enterprise performance and execution of critical business activities within acceptable bounds, or otherwise affect enterprise objectives. Map them to a business-driven hierarchy of risk categories and subcategories (IT risk domains) derived from high-level IT risk scenarios.
   1.6 Break up IT risk by lines of business, product, service and process. Identify potential cascading and coincidental threat types and the probable effect of risk concentration and correlation across silos.
   1.7 Understand how IT capabilities contribute to the enterprise's ability to add value and withstand loss. Compare management's perception of the importance of IT capabilities to their current state.
   1.8 Consider how IT strategies, change initiatives and external requirements may affect the risk profile.
   1.9 Identify risk focus areas, scenarios, dependencies, risk factors and measurements of risk that require management attention and further examination and development.



| Governance Practice | Inputs | | Outputs | |
|---|---|---|---|---|
| | From | Description | Description | To |
| **EDM03.02 Direct risk management.**<br>Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite. | APO12.03 | Aggregated risk profile, including status of risk management actions | Risk management policies | APO12.01 |
| | | | Key objectives to be monitored for risk management | APO12.01 |
| | Outside COBIT | Enterprise risk management (ERM) profiles and mitigation plans | Approved process for measuring risk management | APO12.01 |

**Activities**

1. Promote an IT risk-aware culture and empower the enterprise to proactively identify IT risk, opportunity and potential business impacts.
2. Direct the integration of the IT risk strategy and operations with the enterprise strategic risk decisions and operations.
3. Direct the development of risk communication plans (covering all levels of the enterprise) as well as risk action plans.
4. Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed-on principles of escalation (what to report, when, where and how).
5. Direct that risk, opportunities, issues and concerns may be identified and reported by anyone at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.
6. Identify key goals and metrics of risk governance and management processes to be monitored, and approve the approaches, methods, techniques and processes for capturing and reporting the measurement information.



| Governance Practice | Inputs | | Outputs | |
|---|---|---|---|---|
| | From | Description | Description | To |
| **EDM03.03 Monitor IT risk management.**<br>Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation. | APO12.02 | Risk analysis results | Remedial actions to address risk management deviations | APO12.06 |
| | APO12.04 | Opportunities for acceptance of greater risk | Risk management issues for the board | EDM05.01 |
| | APO12.04 | Review results of third-party risk assessments | | |
| | APO12.04 | Risk analysis and risk profile reports for stakeholders | | |

**Activities**

1 Monitor the extent to which the risk profile is managed within the risk appetite thresholds.

2 Monitor key goals and metrics of risk governance and management processes against targets, analyse the cause of any deviations, and initiate remedial actions to address the underlying causes.

3 Enable review by the key stakeholders of the enterprise's progress toward identified goals.

4 Report any risk management issues to the board or executive committee.

| | | | |
|---|---|---|---|
| APO12 | Manage Risk | Area: | Management |
| | | Domain: | Align, Plan and Organise |

## Process Description

Continually identify, assess and reduce IT-related risks within levels of tolerance set by enterprise executive management.

## Process Purpose Statement

Integrate the management of IT-related enterprise risk with overall enterprise risk management, and balance the costs and benefits of managing IT-related enterprise risks.

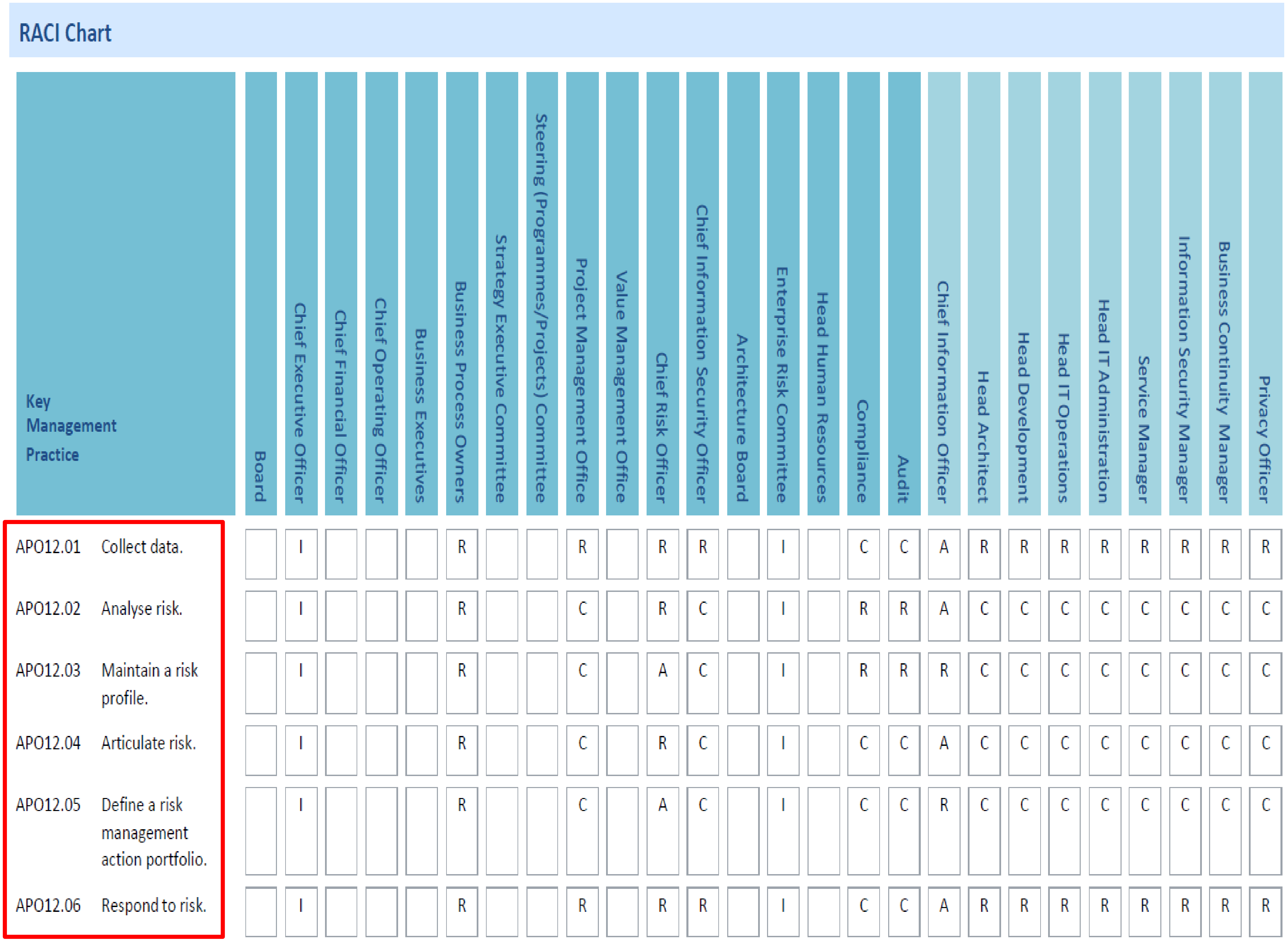
| | | | |
|---|---|---|---|
| APO12 | Manage Risk | Area: | Management |
| | | Domain: | Align, Plan and Organise |

## Process Description

Continually identify, assess and reduce IT-related risks within levels of tolerance set by enterprise executive management.

## Process Purpose Statement

Integrate the management of IT-related enterprise risk with overall enterprise risk management, and balance the costs and benefits of managing IT-related enterprise risks.



## RACI Chart

| Key Management Practice | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Project Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| APO12.01 Collect data. |  | I |  |  |  | R |  |  | R |  | R | R |  | I |  | C | C | A | R | R | R | R | R | R | R | R |
| APO12.02 Analyse risk. |  | I |  |  |  | R |  |  | C |  | R | C |  | I |  | R | R | A | C | C | C | C | C | C | C | C |
| APO12.03 Maintain a risk profile. |  | I |  |  |  | R |  |  | C |  | A | C |  | I |  | R | R | R | C | C | C | C | C | C | C | C |
| APO12.04 Articulate risk. |  | I |  |  |  | R |  |  | C |  | R | C |  | I |  | C | C | A | C | C | C | C | C | C | C | C |
| APO12.05 Define a risk management action portfolio. |  | I |  |  |  | R |  |  | C |  | A | C |  | I |  | C | C | R | C | C | C | C | C | C | C | C |
| APO12.06 Respond to risk. |  | I |  |  |  | R |  |  | R |  | R | R |  | I |  | C | C | A | R | R | R | R | R | R | R | R |

| Management Practice | | Inputs | | Outputs | |
|---|---|---|---|---|---|
| | | From | Description | Description | To |
| APO12.05 | **Define a risk management action portfolio.**<br>Manage as a portfolio opportunities to reduce risk to an acceptable level are . | | | Project proposals for reducing risk | APO02.02;<br>APO13.02 |

## Activities

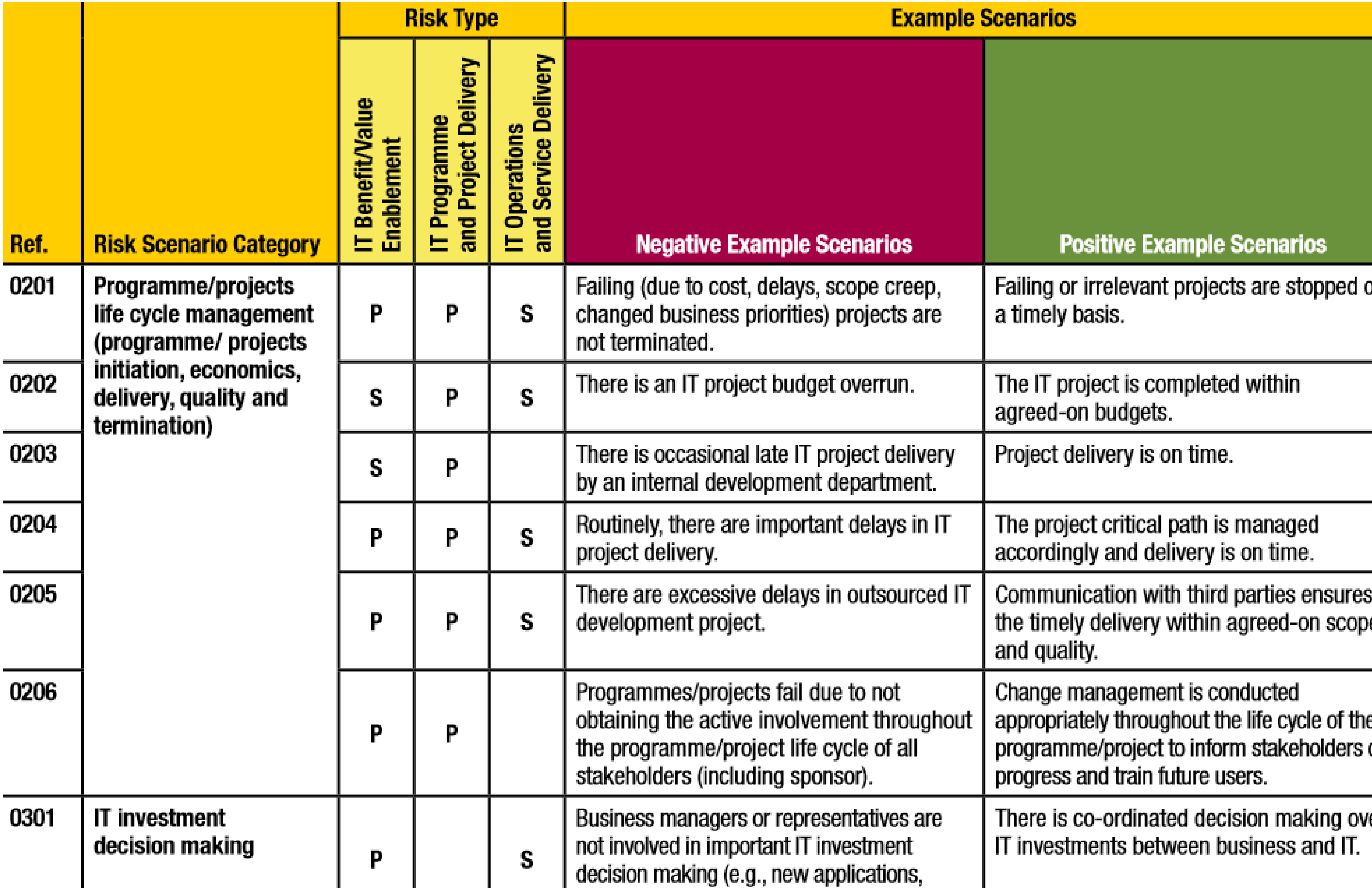
1 Maintain an inventory of control activities that are in place to manage risk and that enable risk to be taken in line with risk appetite and tolerance. Classify control activities and map them to specific IT risk statements and aggregations of IT risk.

2 Determine if each organisational entity monitors risk and accepts accountability for operating within its individual and portfolio tolerance levels.

3 Define a balanced set of project proposals designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering cost/benefits, effect on current risk profile, and regulations.

# RISK SCENARIOS

# 111 risk scenarios



| 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 |
| 0201 | Programme/projects life cycle management (programme/ projects initiation, economics, delivery, quality and termination) | P | P | S | Failing (due to cost, delays, scope creep, changed business priorities) projects are not terminated. | Failing or irrelevant projects are stopped o a timely basis. |
| 0202 |  | S | P | S | There is an IT project budget overrun. | The IT project is completed within agreed-on budgets. |
| 0203 |  | S | P |  | There is occasional late IT project delivery by an internal development department. | Project delivery is on time. |
| 0204 |  | P | P | S | Routinely, there are important delays in IT project delivery. | The project critical path is managed accordingly and delivery is on time. |
| 0205 |  | P | P | S | There are excessive delays in outsourced IT development project. | Communication with third parties ensures the timely delivery within agreed-on scop and quality. |
| 0206 |  | P | P |  | Programmes/projects fail due to not obtaining the active involvement throughout the programme/project life cycle of all stakeholders (including sponsor). | Change management is conducted appropriately throughout the life cycle of the programme/project to inform stakeholders o progress and train future users. |
| 0301 | IT investment decision making | P |  | S | Business managers or representatives are not involved in important IT investment decision making (e.g., new applications, | There is co-ordinated decision making ove IT investments between business and IT. |

# RISK MITIGATION

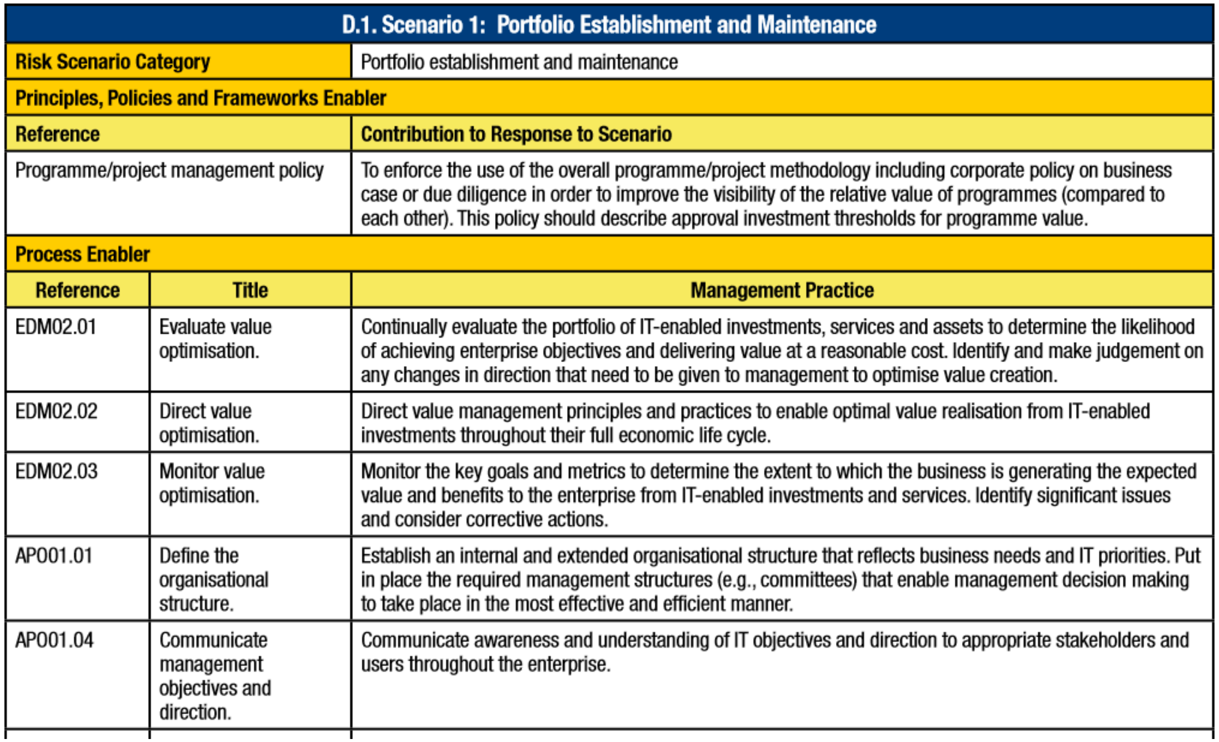
It is possible to identify for any given risk scenario that would exceed risk appetite, a set of COBIT 5 enablers that mitigate the risk scenario.

COBIT 5 enablers:

Process enablers
Organisational structures enablers
Culture, ethics and behavior enablers
Information enablers
Services, infrastructures and applications enablers
People, skills and competencies enablers

# RISK MITIGATION

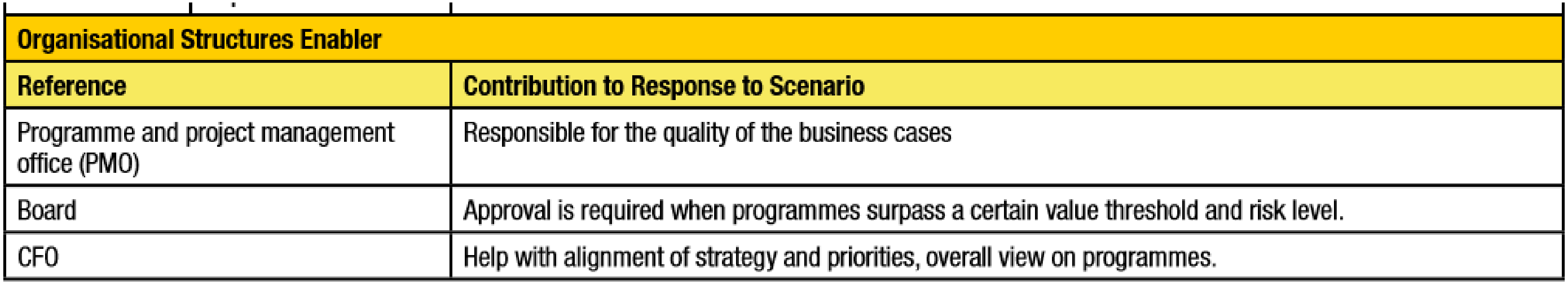
## PROCESS ENABLERS



| D.1. Scenario 1: Portfolio Establishment and Maintenance | | |
|---|---|---|
| **Risk Scenario Category** | | Portfolio establishment and maintenance |
| **Principles, Policies and Frameworks Enabler** | | |
| **Reference** | | **Contribution to Response to Scenario** |
| Programme/project management policy | | To enforce the use of the overall programme/project methodology including corporate policy on business case or due diligence in order to improve the visibility of the relative value of programmes (compared to each other). This policy should describe approval investment thresholds for programme value. |
| **Process Enabler** | | |
| **Reference** | **Title** | **Management Practice** |
| EDM02.01 | Evaluate value optimisation. | Continually evaluate the portfolio of IT-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgement on any changes in direction that need to be given to management to optimise value creation. |
| EDM02.02 | Direct value optimisation. | Direct value management principles and practices to enable optimal value realisation from IT-enabled investments throughout their full economic life cycle. |
| EDM02.03 | Monitor value optimisation. | Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions. |
| APO01.01 | Define the organisational structure. | Establish an internal and extended organisational structure that reflects business needs and IT priorities. Put in place the required management structures (e.g., committees) that enable management decision making to take place in the most effective and efficient manner. |
| APO01.04 | Communicate management objectives and direction. | Communicate awareness and understanding of IT objectives and direction to appropriate stakeholders and users throughout the enterprise. |

# RISK MITIGATION

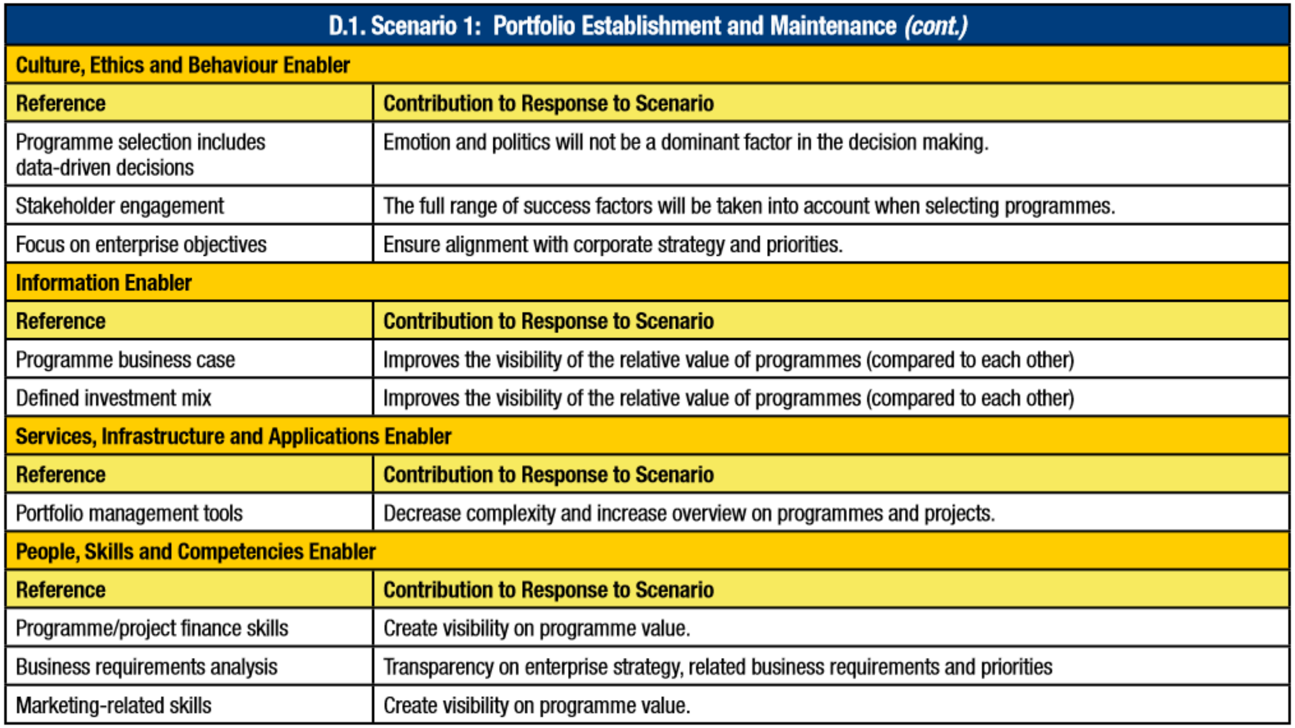
## STRUCTURE ENABLERS



| Organisational Structures Enabler | |
|---|---|
| **Reference** | **Contribution to Response to Scenario** |
| Programme and project management office (PMO) | Responsible for the quality of the business cases |
| Board | Approval is required when programmes surpass a certain value threshold and risk level. |
| CFO | Help with alignment of strategy and priorities, overall view on programmes. |

# RISK MITIGATION

## CULTURE, INFORMATION, SERVICES, PEOPLE ENABLERS



| D.1. Scenario 1: Portfolio Establishment and Maintenance *(cont.)* | |
|---|---|
| **Culture, Ethics and Behaviour Enabler** | |
| **Reference** | **Contribution to Response to Scenario** |
| Programme selection includes data-driven decisions | Emotion and politics will not be a dominant factor in the decision making. |
| Stakeholder engagement | The full range of success factors will be taken into account when selecting programmes. |
| Focus on enterprise objectives | Ensure alignment with corporate strategy and priorities. |
| **Information Enabler** | |
| **Reference** | **Contribution to Response to Scenario** |
| Programme business case | Improves the visibility of the relative value of programmes (compared to each other) |
| Defined investment mix | Improves the visibility of the relative value of programmes (compared to each other) |
| **Services, Infrastructure and Applications Enabler** | |
| **Reference** | **Contribution to Response to Scenario** |
| Portfolio management tools | Decrease complexity and increase overview on programmes and projects. |
| **People, Skills and Competencies Enabler** | |
| **Reference** | **Contribution to Response to Scenario** |
| Programme/project finance skills | Create visibility on programme value. |
| Business requirements analysis | Transparency on enterprise strategy, related business requirements and priorities |
| Marketing-related skills | Create visibility on programme value. |

# The knowing-doing gap

- While organisations do recognise the importance of IT risk governance/management, they are still struggling with getting governance practices implemented and embedded into their organisations (‘knowing-doing gap’)
- Need for an organizational system, i.e. “the way a firm gets its people to work together to carry out the business”. (De Wit and Meyer, 2005).