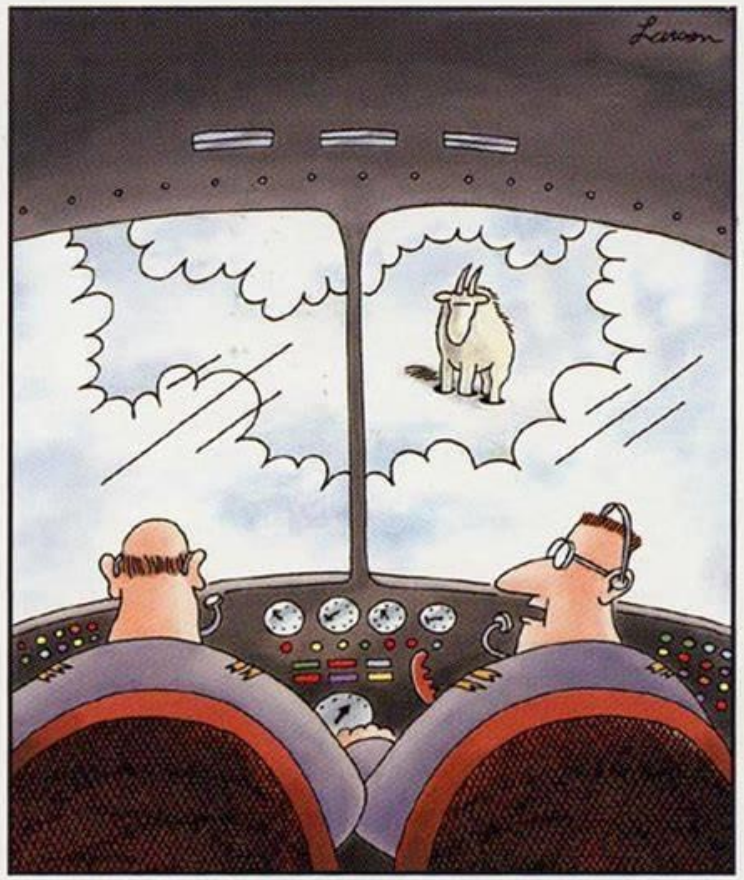
COBIT 2019

COBIT 2019 AND RISK MANAGEMENT

ISACA RISK EVENT 2019, AMSTERDAM, 11 APRIL 2019

OPENING THOUGHTS – THINGS WE DON'T WANT TO HAPPEN WHEN PRACTISING RISK MANAGEMENT

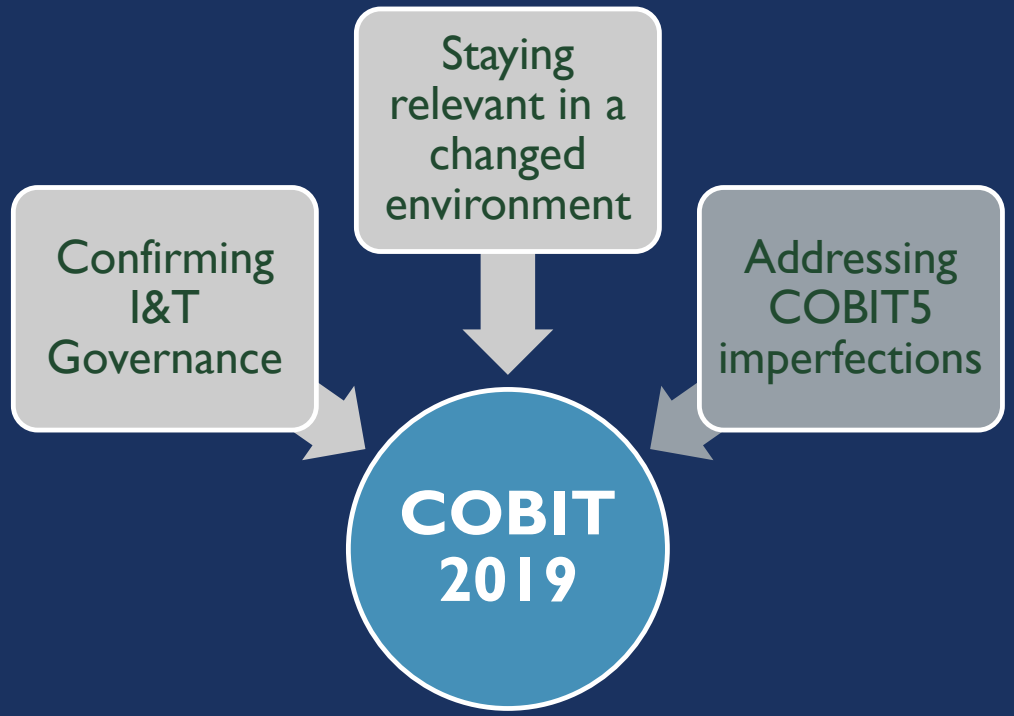


"Say … what's a mountain goat doing way up here in a cloud bank?"

AGENDA

- COBIT 2019 - Why?
- COBIT 2019 – What is new and what has changed?
- COBIT 2019 – how is this relevant for Risk Management
- Q&A

COBIT 2019 – WHY?



THE MAIN DRIVERS FOR THE NEW VERSION OF COBIT

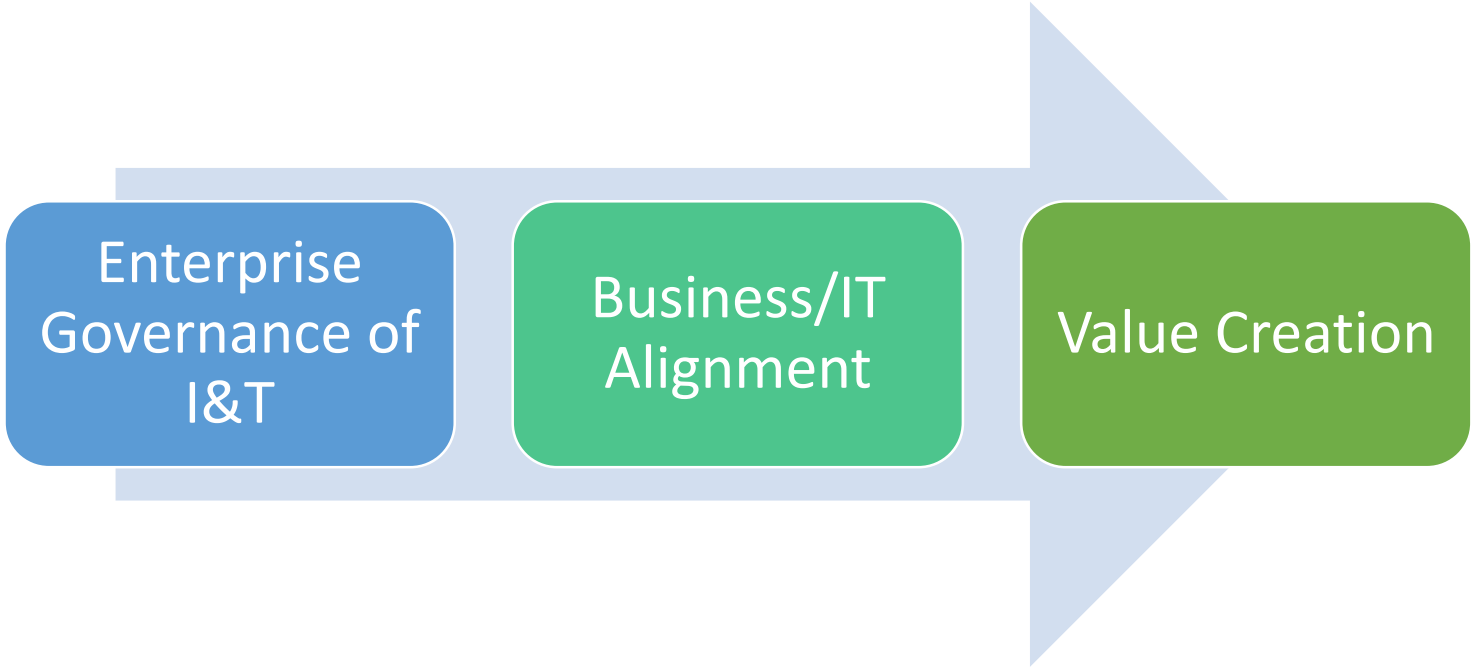
COBIT 2019 – STAYING RELEVANT

- COBIT 5 was published in 2012, making it almost 7 years old..
- New technology and business trends in the use of IT (e.g. digitization, new paradigms) have not been incorporated into COBIT, requiring re-alignment
- The need for the integration of new insights from practitioners, science and academia in the domain of I&T governance creation
- Other standards have evolved, resulting in a different standards/frameworks landscape, requiring a re-alignment
- More fluid, flexible and frequent updates of COBIT required

COBIT 2019
ADDRESSING *COBIT 5* IMPERFECTIONS

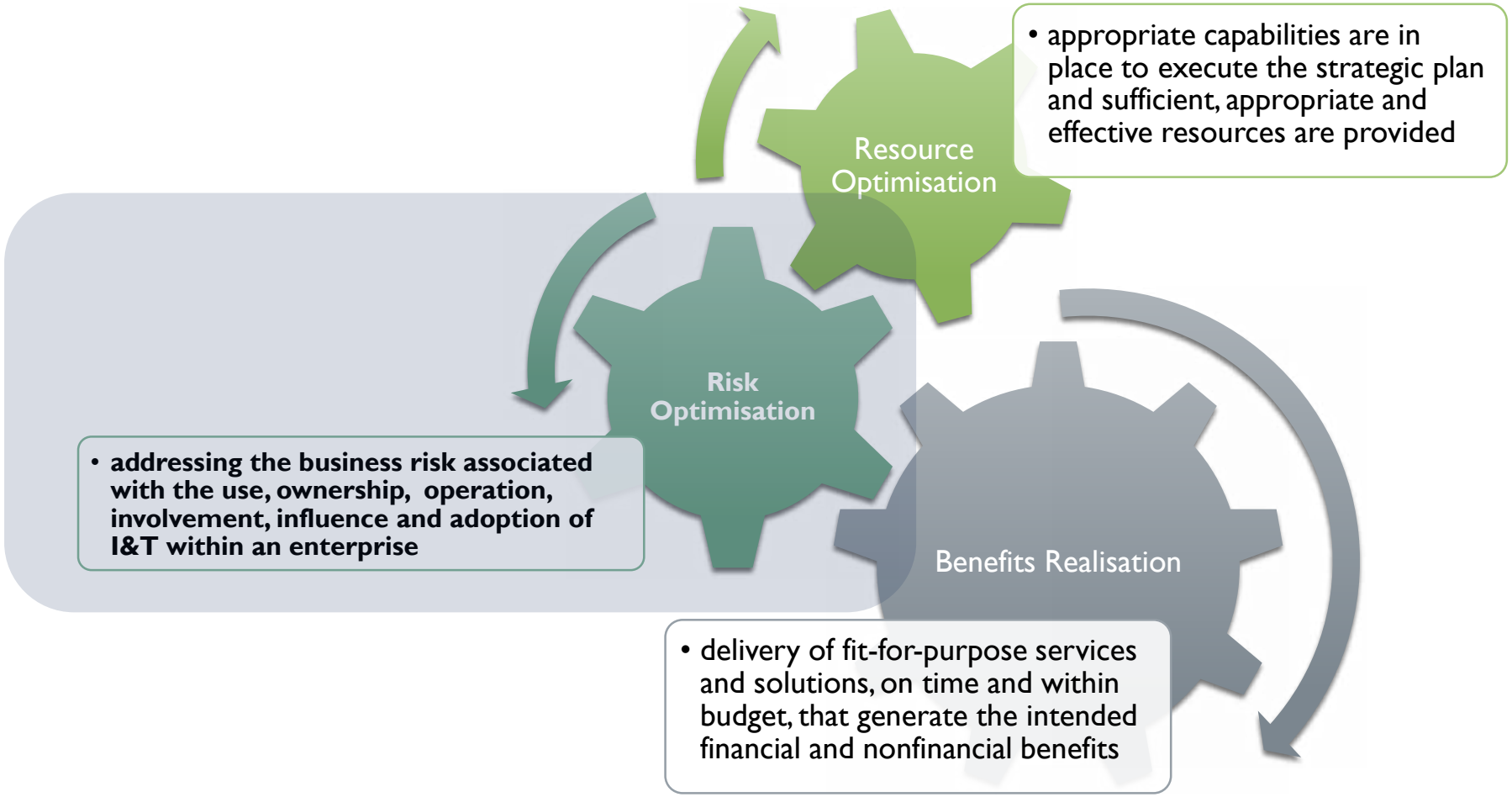
- COBIT users found it hard to locate relevant contents for their needs
- Perceived as complex and challenging to apply in practice
- The enabler model was incomplete in terms of development and guidance, and thus often ignored
- A challenging process capability model and general lack of support of performance management for other enablers
- The perceived reputation of IT governance itself as an inhibitor of change and (administrative) overhead – not per se a COBIT weakness but an IT governance problem at large

COBIT'S PURPOSE: ENTERPRISE GOVERNANCE TO SUPPORT VALUE CREATION



IT - used to refer to the organizational department with main responsibility for technology – versus **I&T** – all the information the enterprise generates, processes and uses to achieve its goals, as well as the technology to support that throughout the enterprise.

COBIT 2019
VALUE DELIVERY

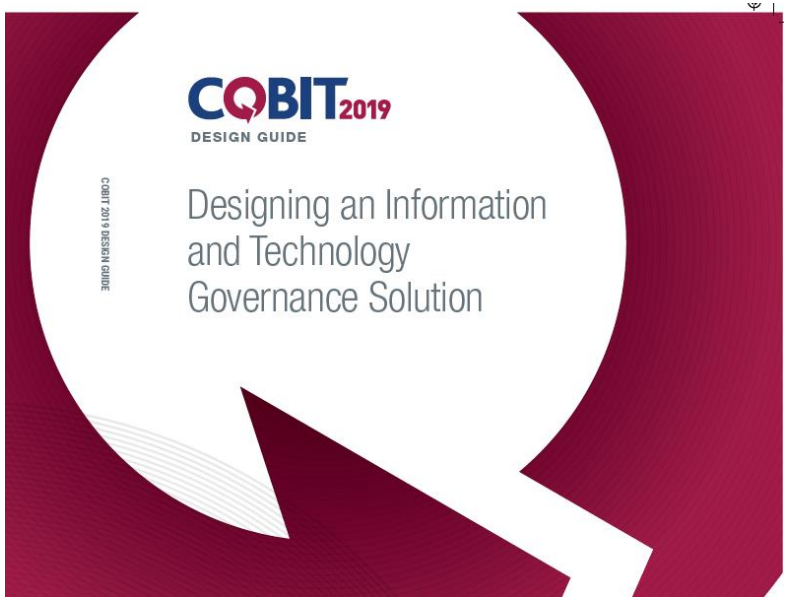


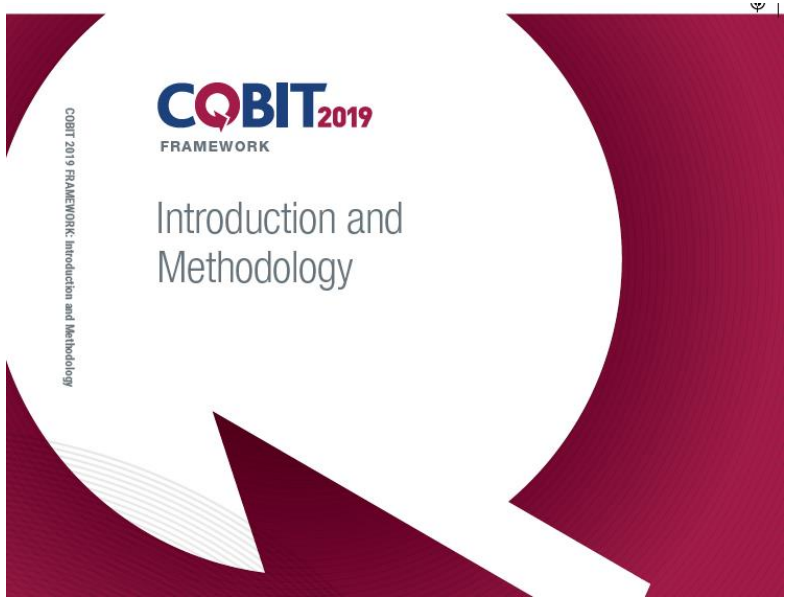
COBIT 2019 – WHAT IS NEW?

NEW AND CHANGED IN COBIT 2019

OVERVIEW COBIT 2019 PRODUCT FAMILY

The COBIT 2019 product family is open-ended. The following publications are now available





COBIT OVERVIEW

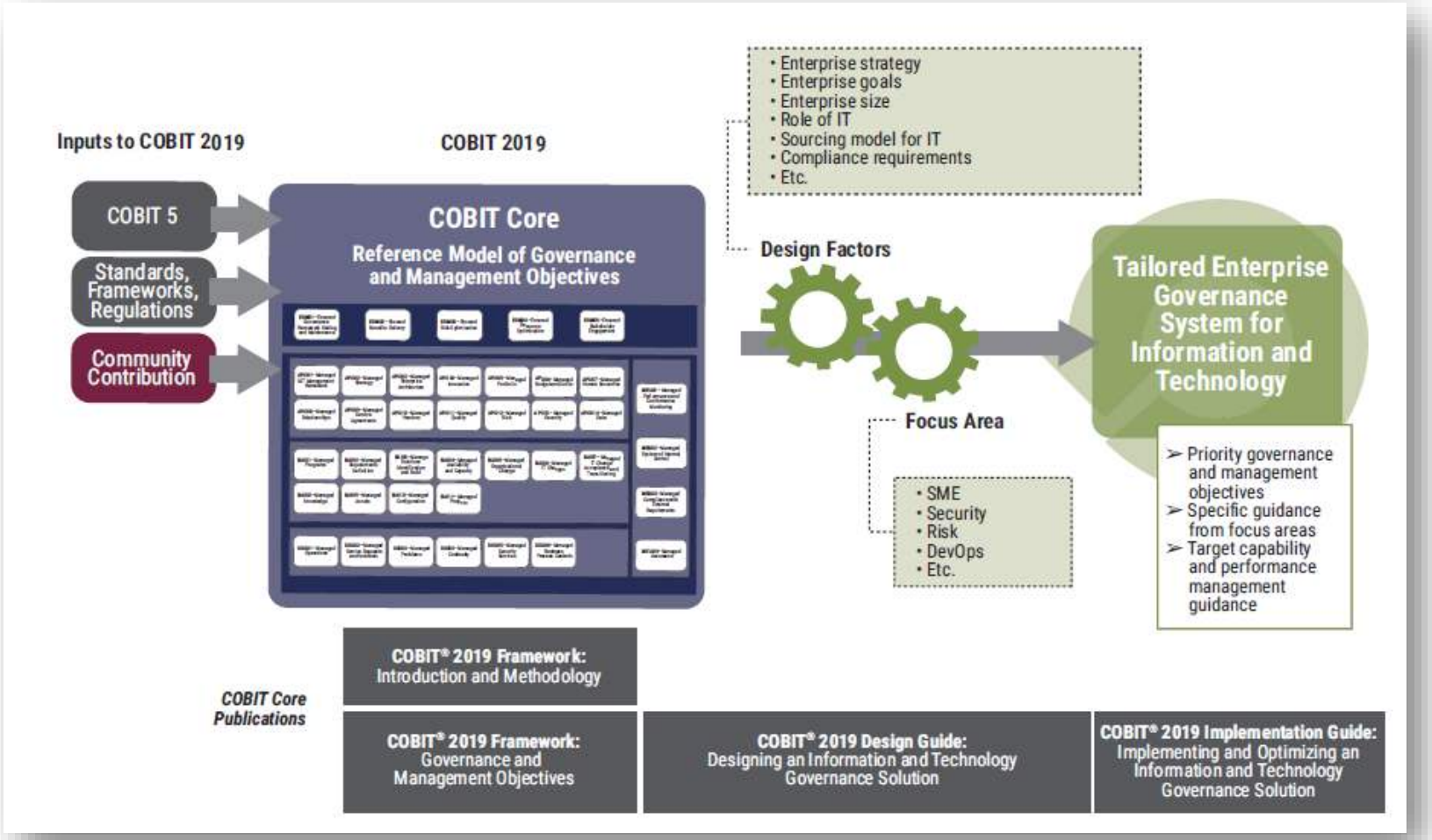
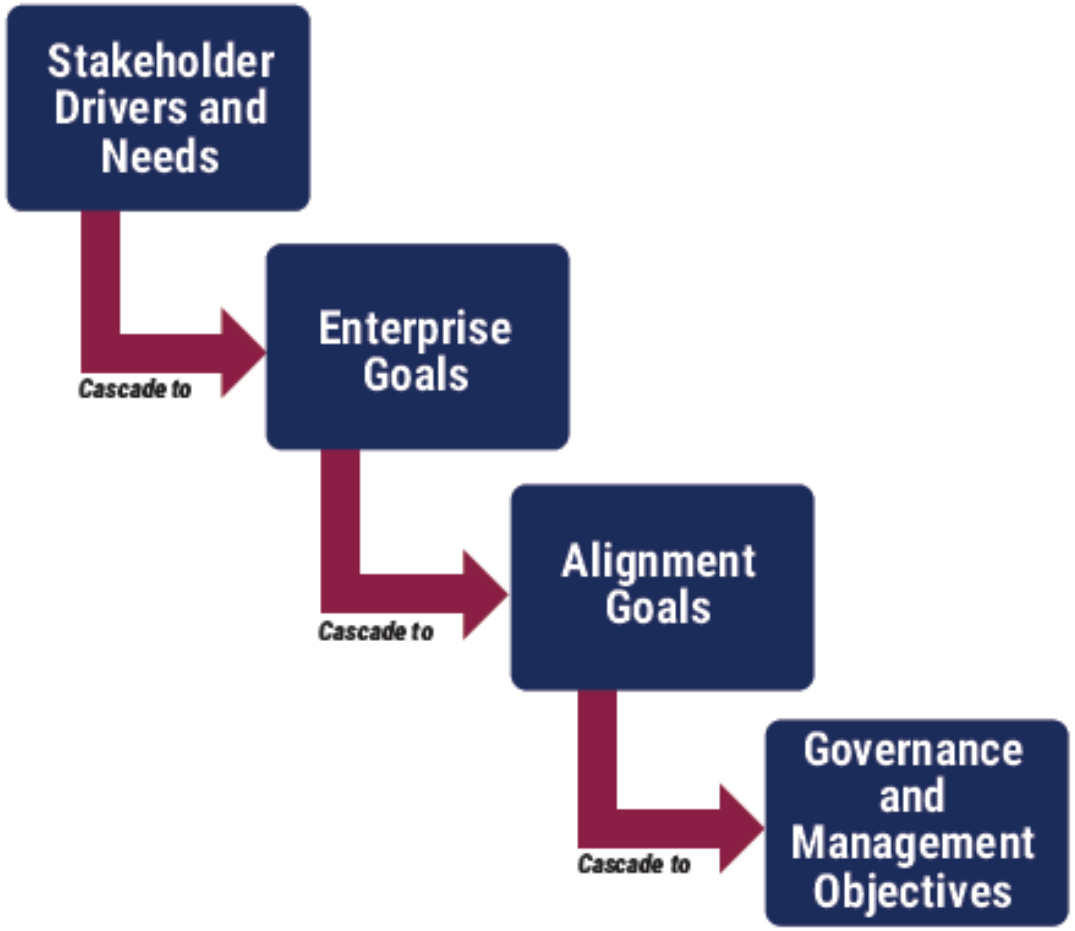
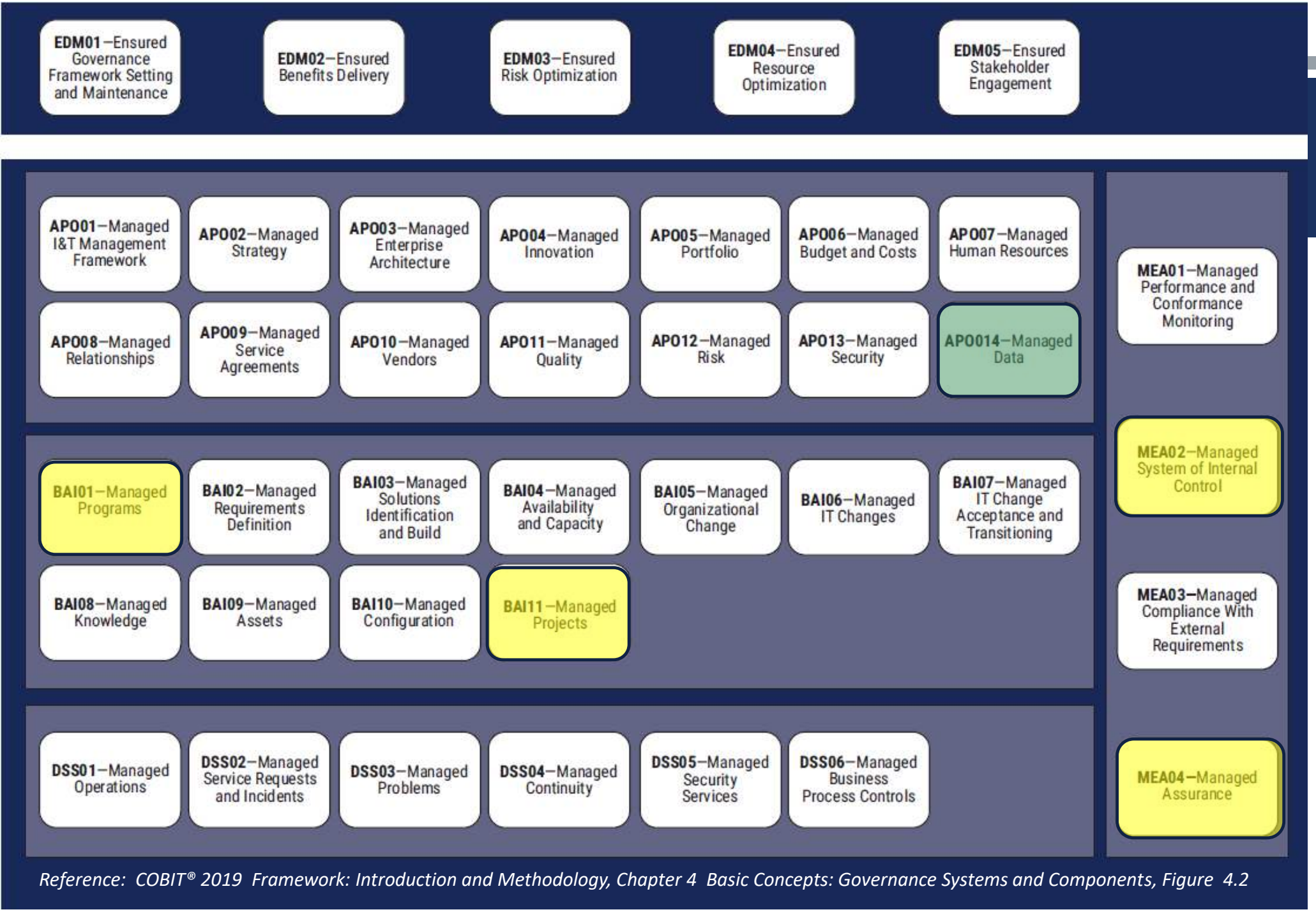


Figure 4.16—COBIT Goals Cascade



COBIT 2019 GOALS CASCADE & GOVERNANCE / MANAGEMENT OBJECTIVES



Reference: COBIT® 2019 Framework: Introduction and Methodology, Chapter 4 Basic Concepts: Governance Systems and Components, Figure 4.2

Known as the Process Reference Model, or PRM in COBIT 5, COBIT® 2019 identifies this as the **COBIT Core Model**.

KEY CONCEPTS - GOVERNANCE AND MANAGEMENT OBJECTIVES

HIGH LEVEL INFORMATION

- Domain name
- Focus area
- Governance or management objective name
- Description
- Purpose statement

GOALS CASCADE

- Applicable Alignment goals
- Applicable Enterprise goals
- Example metrics

RELATED COMPONENTS

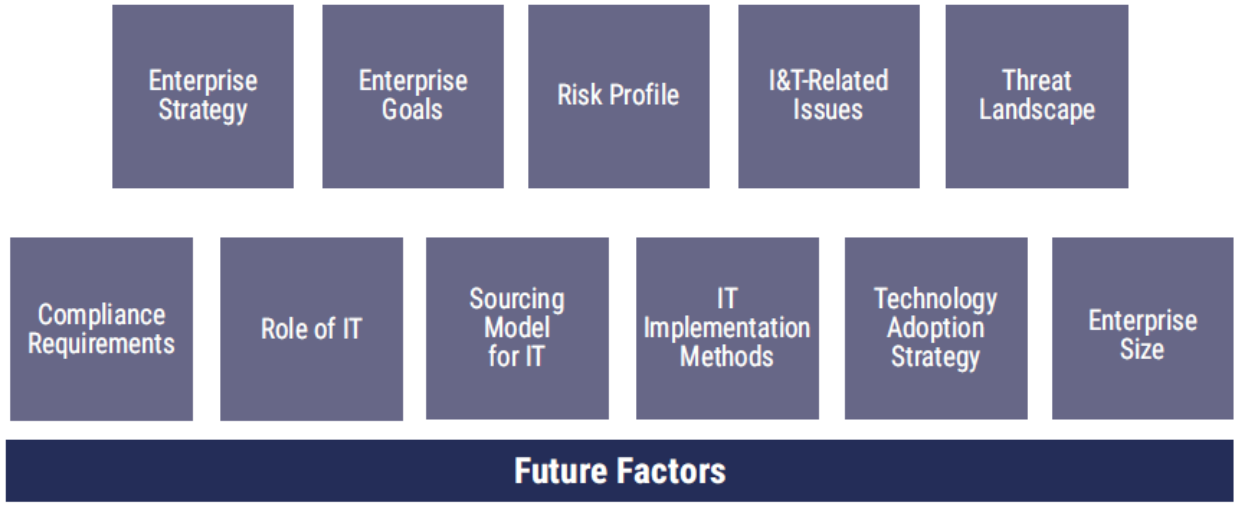
- Processes, practices and activities
- Organizational structures
- Information flows and items
- People, skills and competencies
- Policies and frameworks
- Culture, ethics and behavior
- Services, infrastructure and applications

RELATED GUIDANCE

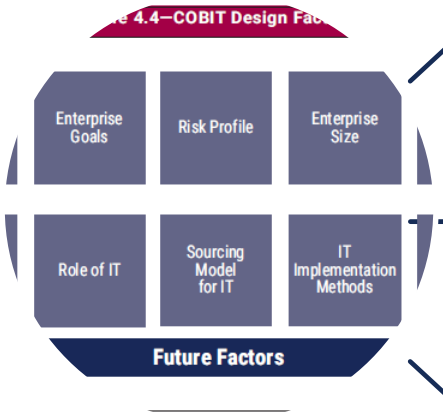
- Where applicable links and cross references are provided to other standards and frameworks for each of the governance components within each governance and management objective

DESIGN FACTORS IN COBIT 2019:

- Influence the design of an enterprise's governance system
- Position it for success in the use of I&T
- More information and detailed guidance on how to use the design factors for designing a governance system can be found in the *COBIT Design Guide* publication



DESIGN FACTORS IN COBIT 2019: EXAMPLES



Enterprise Strategy

- Growth/Acquisition
- Innovation/Differentiation
- Cost Leadership
- Client Service/Stability

Threat Landscape

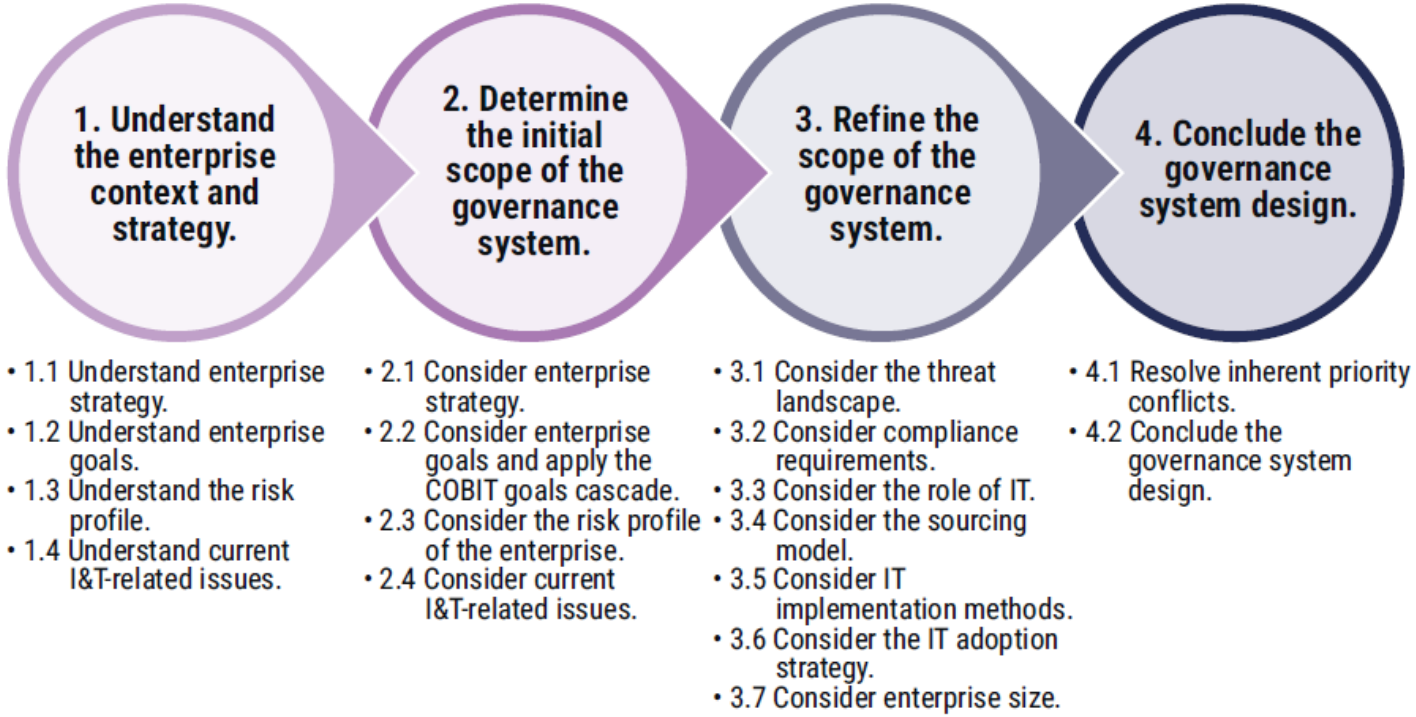
- Normal
- High

Role of IT

- Support
- Factory
- Turnaround
- Strategic

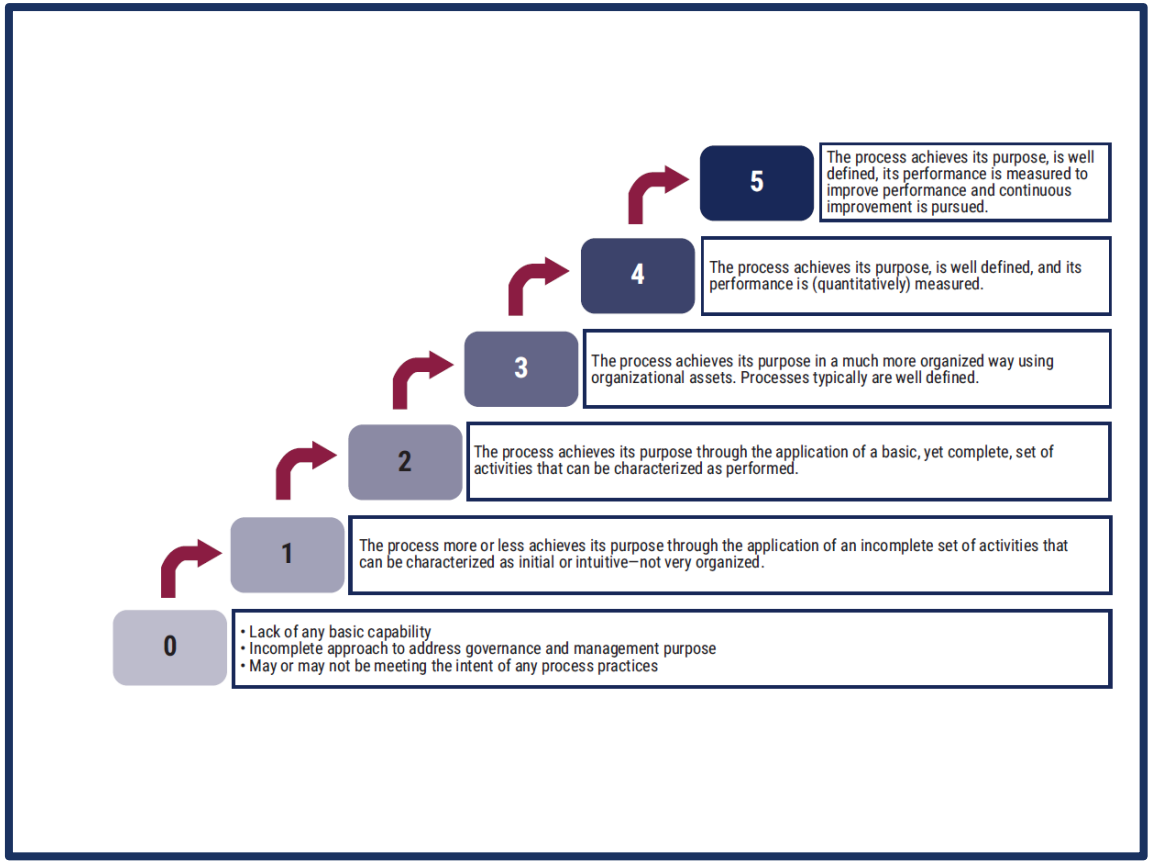
DESIGNING A TAILORED GOVERNANCE SYSTEM
GOVERNANCE SYSTEM DESIGN WORKFLOW

- The different stages and steps in the design process will result in recommendations for prioritizing governance and management objectives or related governance system components, for target capability levels, or for adopting specific variants of a governance system component.



Reference: COBIT® 2019 Framework: Introduction and Methodology, Chapter 7 Designing a Tailored Governance System, Figure 7.2

PERFORMANCE MANAGEMENT IN COBIT 2019 – PROCESS CAPABILITY LEVELS



- COBIT 2019 supports a CMMI-based process capability scheme
- The process within each governance and management objective can operate at capability levels, between 0 to 5
- The capability level is a measure for how well a process is implemented and performing
- Each process **activity** is associated with a capability level

WHAT IS COBIT AND WHAT IT IS NOT: SETTING THE RIGHT EXPECTATIONS

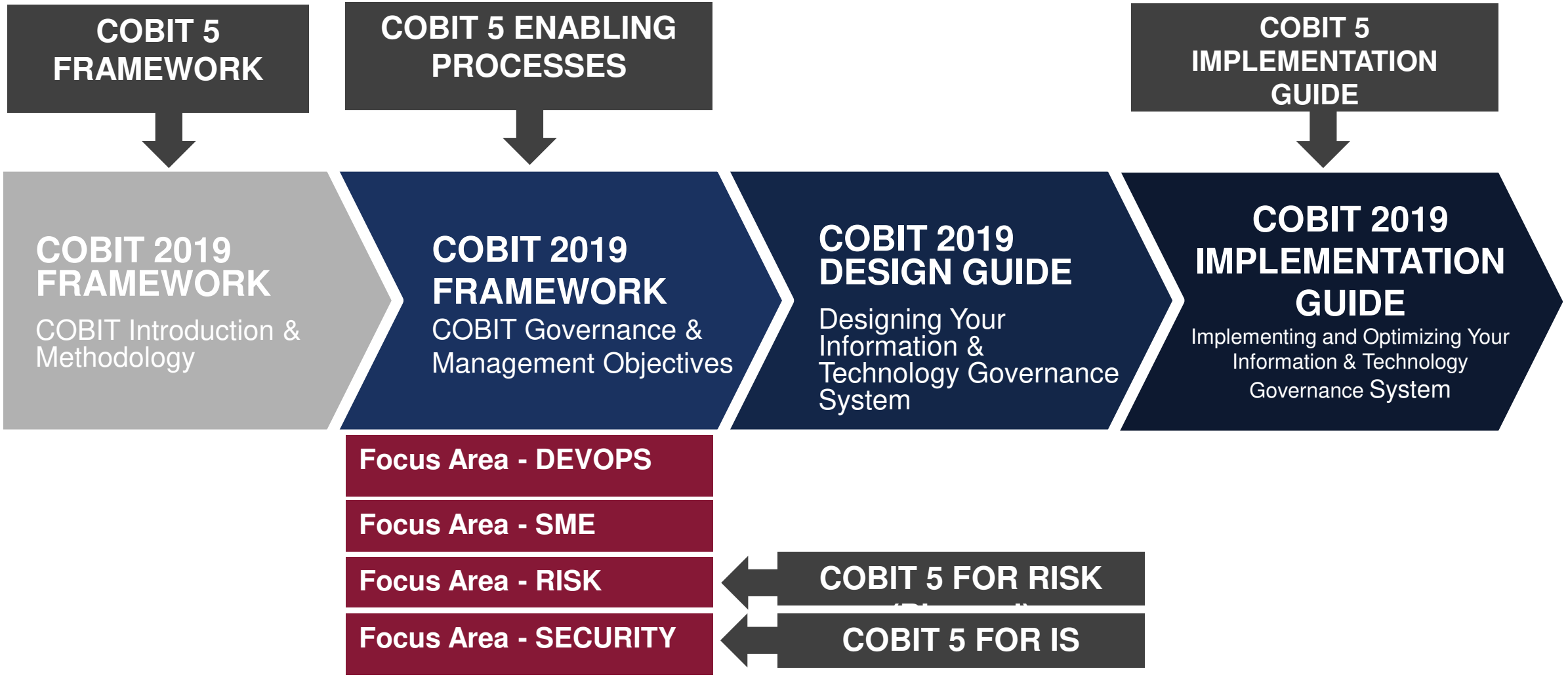
COBIT IS

- A framework for the governance and management of enterprise I&T
- COBIT defines the components to build and sustain a governance system
- COBIT defines the design factors that should be considered by the enterprise to build a best fit governance system, including risk
- COBIT is flexible and allows guidance on new topics to be added

COBIT IS NOT

- A full description of the whole IT environment of an enterprise
- A framework to organize business processes
- An (IT-) technical framework to manage all technology
- COBIT does not make or prescribe any IT-related decisions, e.g. sourcing strategies, technology choices, …

MAJOR DIFFERENCES - ALIGNMENT TO COBIT 5



COBIT 2019 AND RISK MANAGEMENT

WHAT IS MOST RELEVANT IN COBIT 2019 FOR RISK MANAGEMENT?

COBIT 2019 AND RISK MANAGEMENT (NOW AND UPCOMING)

- COBIT 2019 integrates risk governance and management with overall I&T governance and management.
- COBIT 2019 provides the hooks for more detailed and technical guidance beyond the scope of COBIT.
- COBIT 2019 includes integrated process capability assessment, based on CMMI
- COBIT 2019 has updated the generic risk scenarios to support management efforts

- The COBIT Core Model contains specific risk governance & management objectives, with supporting processes:
  - EDM03-Ensured Risk Optimisation
  - APO12—Managed Risk
- Specific Org.anisational Structures, Skills, Culture aspects, etc. are described as well
- *Detailed focus area guidance will be available soon for information security and I&T risk.*

COBIT 2019 AND RISK MANAGEMENT – *EDM03 – ENSURED RISK OPTIMISATION* AND *APO12 – MANAGED RISK*

EDM03

A. Component: Process	
Governance Practice	**Example Metrics**
EDM03.01 Evaluate risk management. Continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.	a. Level of unexpected enterprise impact b. Percent of I&T risk that exceeds enterprise risk tolerance c. Refreshment rate of risk factor evaluation
Activities	**Capability Level**
1. Understand the organization and its context related to I&T risk.	2
2. Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.	
3. Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.	
4. Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.	
5. Proactively evaluate I&T risk factors in advance of pending strategic enterprise decisions and ensure that risk considerations are part of the strategic enterprise decision process.	3
6. Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.	
7. Attract and maintain necessary skills and personnel for I&T Risk Management	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16

APO12

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO12.02 Analyze risk. Develop a substantiated view on actual I&T risk, in support of risk decisions.	a. Number of identified I&T risk scenarios b. Time since last update of I&T risk scenarios
Activities	**Capability Level**
1. Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of assets.	3
2. Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop expectations for specific control activities and capabilities to detect.	
3. Estimate the frequency (or likelihood) and magnitude of loss or gain associated with I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.	
4. Compare current risk (I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or elevated risk.	
5. Propose risk responses for risk exceeding risk appetite and tolerance levels.	
6. Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.	
7. Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise requirements and verify that estimations were properly calibrated and scrutinized for bias.	4
8. Analyze cost/benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.	5

COBIT 2019 AND RISK MANAGEMENT: DESIGN FACTORS – RISK PROFILE

- The risk profile identifies the sort of IT-related risk to which the enterprise is currently exposed and indicates which areas of risk are exceeding the risk appetite.
- The risk categories listed in **figure 2.7** merit consideration

Figure 2.7—Risk Profile Design Factor (IT Risk Categories)

Reference	Risk Category	Example Risk Scenarios
1	IT-investment decision making, portfolio definition and maintenance	A. Programs selected for implementation misaligned with corporate strategy and priorities B. Failure of IT-related Investments to support digital strategy of the enterprise C. Selection of wrong software (in terms of cost, performance, features, compatibility, redundancy, etc.) for acquisition and implementation D. Selection of wrong infrastructure (in terms of cost, performance, features, compatibility, etc.) for implementation E. Duplication or important overlaps between different investment initiatives F. Long-term incompatibility between new investment programs and enterprise architecture G. Misallocation, inefficient management and/or competition for resources without alignment to business priorities
2	Program and projects lifecycle management	A. Failure of senior management to terminate failing projects (due to cost explosion, excessive delays, scope creep, changed business priorities) B. Budget overruns for I&T projects C. Lack of quality of I&T projects D. Late delivery of I&T projects E. Failure of third-party outsourcers to deliver projects as per contractual agreements (any combination of exceeded budgets, quality problems, missing functionality, late delivery)
3	IT cost and oversight	A. Extensive dependency on, and use of, user-created, user-defined, user-maintained applications and *ad hoc* solutions B. Excess cost and/or ineffectiveness of I&T-related purchases outside of the I&T procurement process C. Inadequate requirements leading to ineffective Service Level Agreements (SLAs) D. Lack of funds for I&T related investments

COBIT 2019 AND RISK MANAGEMENT: DESIGN FACTORS – RISK PROFILE

- The risk profile identifies the sort of IT-related risk to which the enterprise is currently exposed and indicates which areas of risk are exceeding the risk appetite.
- The risk categories listed in **figure 2.7** merit consideration

Figure 2.7—Risk Profile Design Factor (IT Risk Categories) *(cont.)*

Reference	Risk Category	Example Risk Scenarios
11	Logical attacks (hacking, malware, etc.)	A. Unauthorized (internal) users trying to break into systems B. Service interruption due to denial-of-service (DoS) attack C. Website defacement D. Malware attack E. Industrial espionage F. Hacktivism G. Disgruntled employee implements a time bomb which leads to data loss H. Company data stolen through unauthorized access gained by a phishing attack I. Foreign government attacks on critical systems
12	Third-party/supplier incidents	A. Inadequate performance of outsourcer in large-scale, long-term outsourcing arrangement (e.g., through lack of supplier due diligence regarding financial viability, delivery capability and sustainability of supplier's service) B. Accepting unreasonable terms of business from IT suppliers C. Inadequate support and services delivered by vendors, not in line with SLA D. Noncompliance with software license agreements (use and/or distribution of unlicensed software) E. Inability to transfer to alternative suppliers due to overreliance or overdependence on current supplier F. Purchase of IT services (especially cloud services) by the business without consultation /involvement of IT, resulting in inability to integrate the service with in-house services. G. Inadequate or unenforced SLA to obtain agreed services and penalties in case of noncompliance

COBIT 2019 AND RISK MANAGEMENT: DESIGN FACTORS – I&T ISSUES

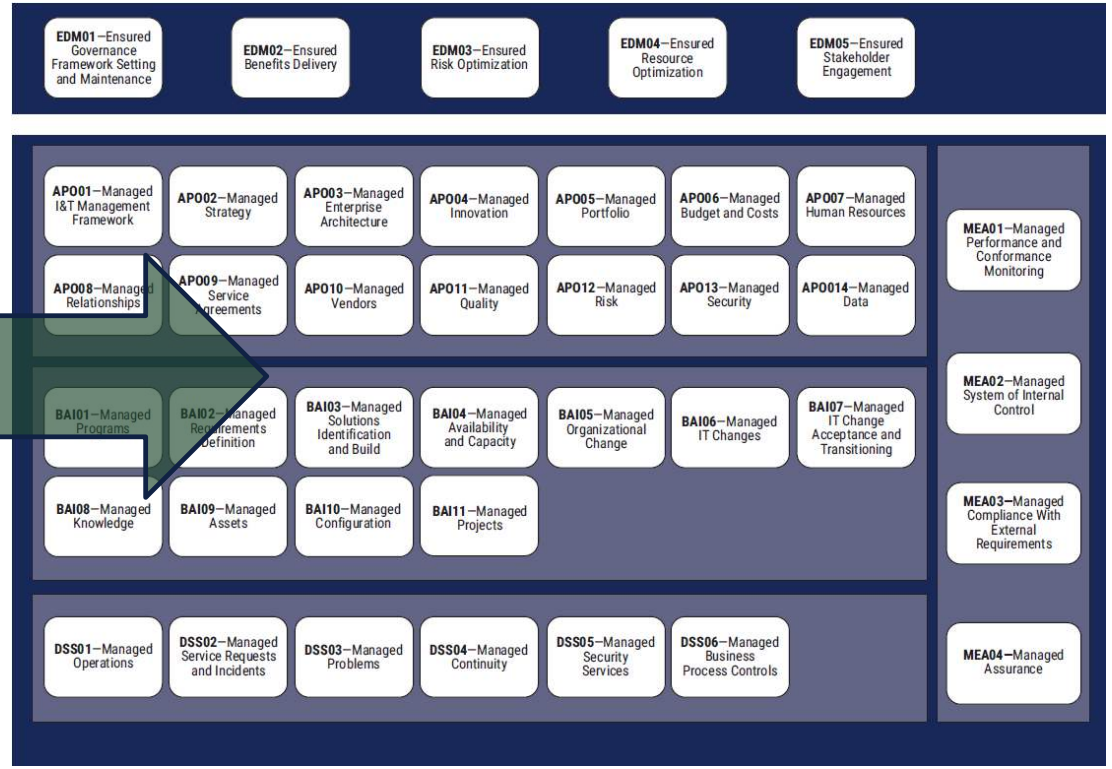
- A related method for an I&T risk assessment for the enterprise is to consider which I&T-related issues it currently faces, or, in other words, what I&T-related risk has materialized.
- The most common of such issues are listed in figure 2.8

Figure 2.8—I&T-Related Issues Design Factor	
Reference	**Description**
A	Frustration between different IT entities across the organization because of a perception of low contribution to business value
B	Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value
C	Significant I&T related incidents, such as data loss, security breaches, project failure, application errors, etc. linked to IT
D	Service delivery problems by the IT outsourcer(s)
E	Failures to meet IT related regulatory or contractual requirements
F	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems
G	Substantial hidden and rogue IT spending, i.e., I&T spending by user departments outside the control of the normal I&T investment decision mechanisms and approved budgets
H	Duplications or overlaps between various initiatives or other forms of wasting resources
I	Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction
J	IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget
K	The Board members, executives or senior management are reluctant to engage with I&T, or there is a lack of committed business sponsors for I&T

COBIT 2019 AND RISK MANAGEMENT: MAPPING RISK & ISSUES WITH GOVERNANCE AND MANAGEMENT OBJECTIVES

Figure 2.7—Risk Profile Design Factor (IT Risk Categories)

Reference	Risk Category	Example Risk Scenarios
1	IT-investment decision making, portfolio definition and maintenance	A. Programs selected for implementation misaligned with corporate strategy and priorities B. Failure of IT-related Investments to support digital strategy of the enterprise C. Selection of wrong software (in terms of cost, performance, features, compatibility, redundancy, etc.) for acquisition and implementation D. Selection of wrong infrastructure (in terms of cost, performance, features, compatibility, etc.) for implementation E. Duplication or important overlaps between different investment initiatives F. Long-term incompatibility between new investment programs and enterprise architecture G. Misallocation, inefficient management and/or competition for resources without alignment to business priorities
2	Program and projects lifecycle management	A. Failure of senior management to terminate failing projects (due to cost explosion, excessive delays, scope creep, changed business priorities) B. Budget overruns for I&T projects C. Lack of quality of I&T projects D. Late delivery of I&T projects E. Failure of third-party outsourcers to deliver projects as per contractual agreements (any combination of exceeded budgets, quality problems, missing functionality, late delivery)
3	IT cost and oversight	A. Extensive dependency on, and use of, user-created, user-defined, user-maintained applications and *ad hoc* solutions B. Excess cost and/or ineffectiveness of I&T-related purchases outside of the I&T procurement process C. Inadequate requirements leading to ineffective Service Level Agreements (SLAs) D. Lack of funds for I&T related investments



COBIT 2019: IN CONCLUSION…

WHY COBIT 2019?

GENERALLY ACCEPTED, BUSINESS FRAMEWORK FOR IT, USED AND USEABLE BY BUSINESS/ASSURANCE / RISK MANAGEMENT

'PLAYS WELL WITH OTHERS', I.E. ALIGNS WITH OTHER FRAMEWORKS, CAN BE COMPLEMENTED WITH MISSING BITS & PIECES, E.G. FOR QUANTITATIVE RISK ANALYSIS

STRUCTURED FROM BEGINNING TO END

CAN BE TAILORED TO SPECIFIC ENTERPRISE NEEDS THANKS TO THE (NEW) DESIGN FACTORS, WHICH INCLUDE RISK PROFILE AND IT ISSUES AN ORGANISATION IS FACED WITH

INCLUDES INTEGRATED PERFORMANCE MANAGEMENT FEATURES – CAPABILITY LEVELS, METRICS AT DIFFERENT LEVELS, ALLOWING TO SET TARGETS AND TO MEASURE TARGETS

IS OPEN AND FREELY AVAILABLE, NOT PROPRIETARY HENCE NO LOCK-INS OR IMPORTANT IP INVESTMENTS…

WHY COBIT 2019 FOR RISK MANAGEMENT? WHAT'S IN THE COBIT TOOLBOX?

- Risk Governance and Risk management objectives and processes are spelled out and can be implemented at different and evolving capability levels
  - The Performance management system for these processes allows to measure and adjust them to target
- Design Factors (Risk Profile, IT Issues, threat landscape, …) allow to design the governance process taking into account risk factors
  - The updated list with Generic Risk Scenarios is a valuable tool for validation of an organisation's own risk register
- Mapping between Risk Scenarios and Governance and Management Objectives , aka 'controls', allows more reliable risk assessment and better risk response, whilst saving on the need to identify controls for each new risk
  - Performance monitoring for those 'controls' is provided through the process capability scheme
- Definition of relevant information items for risk management → risk profile, risk register, …
- Designated focus area guidance for information security, information risk management is under development, other areas will be planned
- COBIT has attention for 'non-process' related guidance as well

IS COBIT 2019 PERFECT FOR RISK MANAGEMENT?

- I would love to say yes ☺
- But…
  - COBIT does not include technical risk guidance (but all of that can be made to fit under COBIT)
  - COBIT does not include risk taxonomies (or ontology as some would say) nor does it prescribe risk assessment methodologies (although we provide recommendations on the requirements for such methods)
  - And as soon as you start using COBIT you will probably discover more…

OBSERVED PAIN POINTS WITH IT RISK MANAGEMENT COBIT CAN (PARTIALLY) HELP TO SOLVE…

- Suboptimal organisation within enterprises – overall responsibility is not assigned, or is assigned at too low levels in the hierarchy; risk management is organised in very fragmented ways, e.g. per risk type and often incomplete in scope
- Widespread confusion between *risk management* and *controls (compliance) monitoring*
- Lack of involvement of senior management, triggered by often perceived or assumed conflict between risk management and performance
- Quality of risk assessments – inconsistent methods for risk identification and risk assessment are used throughout an organisation, often aggravated by a lack of (decent) risk taxonomy and clearly defined risk appetite.
- Inadequate incentives setting for desired (well, from a good risk management standpoint) risk management behaviours

CLOSING THOUGHTS

Despite what one would sometimes hope, risk always exists, whether or not it is detected or recognised by an organisation…

COBIT 2019 AND RISK

Q&A