Introduction to COBIT 5

Executive Summary

Information is a key resource for all enterprises, and from the time that information is created to the moment that it is destroyed, technology plays a significant role. Information technology is increasingly advanced and has become pervasive in enterprises and in social, public and business environment.

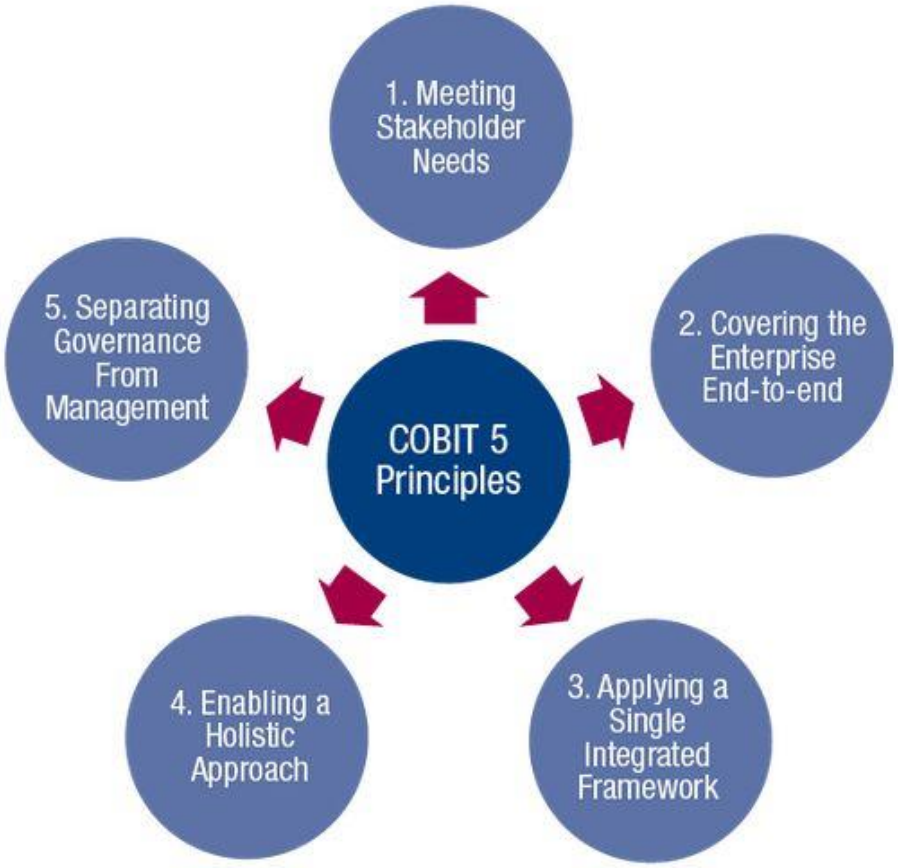
As a result, today, more than ever, enterprises and their executives strive to:

- Maintain high-quality information to support business decisions.
- Generate business value from IT-enabled investment, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT.
- Achieve operational excellence through the reliable and efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimise the cost of IT services and technology.
- Comply with ever-increasing relevant laws, regulations, contractual agreement and policies.

Over the past decade, the term 'governance' has moved to the forefront of business thinking in response to examples demonstrating the importance of good governance and, on the other end of the scale, global business mishaps.

Successful enterprises have recognised that the board and executives need to embrace IT like any other significant part of doing business. Boards and management—both in the business and IT functions—must collaborate and world together, so that IT is included within the governance and management approach. In addition, legislation is increasingly being passed and regulations implemented to address this~

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.



COBIT 5 is based on five key principles (shown above) for governance and management of enterprise IT:

1. **Principle 1: Meeting Stakeholder Needs**—Enterprises exist to create value for their stakeholders by maintaining a balance between the realisation of benefits and the optimisation of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customise COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific IT-related goals and mapping these to specific processes and practices.
2. **Principle 2: Covering the Enterprise End-to-end**—COBIT 5 integrates governance of enterprise IT into enterprise governance:
    a. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the IT function, but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.
    b. It considers all IT-related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone—internal and external—that is relevant to governance and management of enterprise information and related IT.
3. **Principle 3: Applying a Single, Integrated Framework**—There are many IT-related standards and good practices, each providing guidance on a subset of IT activities. COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT.

4. **Principle 4: Enabling a Holistic Approach**—Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting component. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise. The COBIT 5 framework defines seven categories of enablers:
    a. Principles, Policies and Frameworks
    b. Processes
    c. Organisational Strudures
    d. Culture, Ethics and Behaviour
    e. Information
    f. Services, Infrastructure and Applications
    g. People, Skills and Competencies
5. **Principle 5: Separating Governance from Management**—The COBIT 5 framework makes a clear distinction between governance and management These two disciplines encompass different types of activities, require different organisational structures and serve different purposes. COBIT 5's view on this key distinction between governance and management is:
    a. Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organisational structures at an appropriate level, particularly in large, complex enterprises.
    b. Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the thief executive officer (CEO).

Together, these five principles enable the enterprise to build an effective governance and management framework that optimises information and technology investment and use for the benefit of stakeholders.

Overview

COBIT 5 provides the next generation of ISACAs guidance on the enterprise governance and management of IT. It builds on more than 15 years of practical usage and application of COBIT by many enterprises and users from business, IT, risk, security and assurance communities. The major drivers for the development of COBIT 5 include the need to:

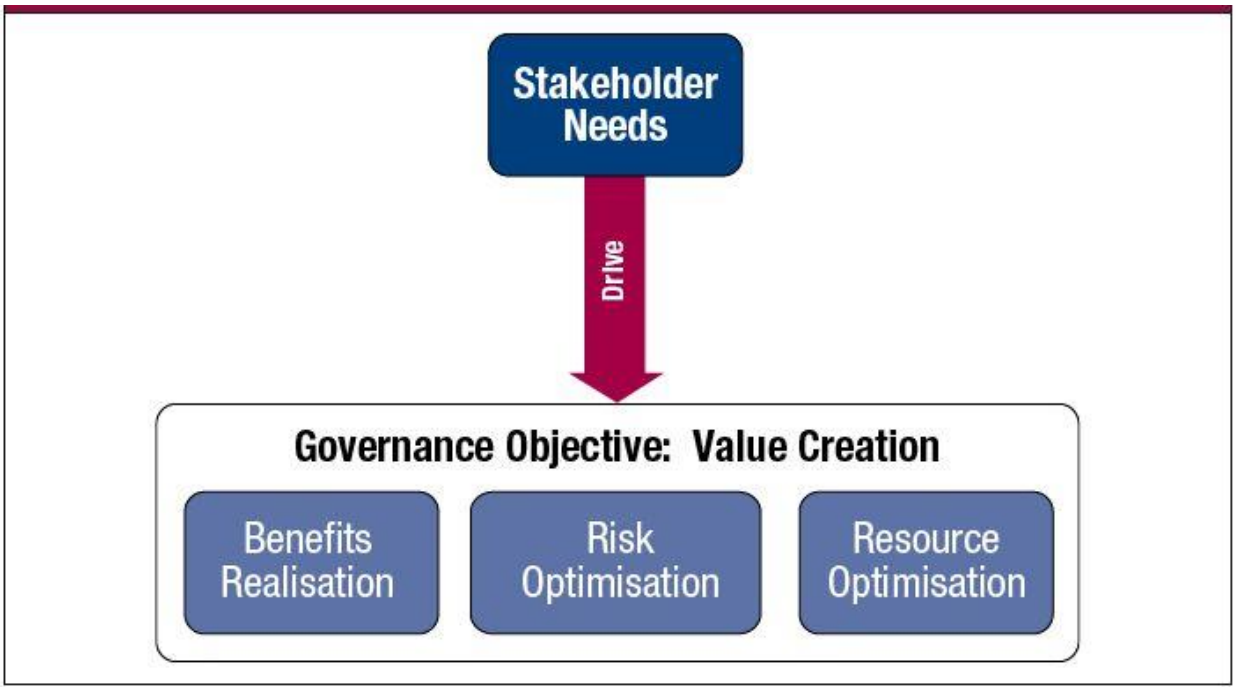
- Provide more stakeholders a say in determining what they expect from information and related technology (what benefits at what acceptable level of risk and at what costs) and what their priorities are in ensuring that expected value is actually being delivered. Some will want short-term returns and others long-term sustainability. Some will be ready to take a high risk that others will not. These divergent and sometimes conflicting expeditions need to be dealt with

effectively. Furthermore, not only do these stakeholders want to be more involved, but they want more transparency regarding how this will happen and the actual results achieved.

- Address the increasing dependency of enterprise success on external business and IT parties such as outsourcers, suppliers, consultant, clients, cloud and other service providers, and on a diverse set of internal means and mechanisms to deliver the expected value
- Deal with the amount of information, which has increased significantly. How do enterprises select the relevant and credible information that will lead to effective and efficient business decisions? Information also needs to be managed effectively and an endive information model can assist
- Deal with much more pervasive IT; it is more and more an integral part of the business. Often, it is no longer satisfactory to have IT separate even if it is aligned to the business. It needs to be an integral part of the business projects, organisational structures, risk management policies, skills, processes, etc. The roles of the chief information officer (CIO) and the IT function are evolving. More and more people within the business functions have IT skills and are, or will be, involved in IT decisions and IT operations. IT and business will need to be better integrated.
- Provide further guidance in the area of innovation and emerging technologies; this is about creativity, inventiveness, developing new products, making the existing products more compelling to customers and reaching new types of customers. Innovation also implies streamlining product development manufacturing and supply chain processes to deliver products to market with increasing levels of efficiency, speed and quality.
- Cover the full end-to-end business and IT functional responsibilities, and cover all aspects that lead to effective governance and management of enterprise IT, such as organisational structures, politics and culture, over and above processes
- Get better control over increasing user-initiated and user-controlled IT solutions
- Achieve enterprise:
    - Value creation through effective and innovative use of enterprise IT
    - Business user satisfaction with IT engagement and services
    - Compliance with relevant laws, regulations, contractual agreement and internal policies
    - Improved relations between business needs and IT objectives
- Connect to, and, where relevant, align with, other major frameworks and standards in the marketplace, such as Information Technology Infrastructure Library (ITILO), The Open Group Architecture Forum (TOGAF), Project Management Body of Knowledge (PMBOKOD), PRojects IN Controlled Environment 2 (PRINCE.), Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the International Organization for Standardization (ISO) standards. This will help stakeholders understand how various frameworks, good practices and standards are positioned relative to each other and how they can be used together.
- Integrate all major ISACA frameworks and guidance, with a primary focus on COBIT, Val IT and Risk but also considering the Business Model for Information Security (BMIS), the IT Assurance Framework (ITAF), the publication titled Board Briefing on IT Governance, and the Taking Governance Forward (TGF) resource, such that COBIT 5 covers the complete enterprise and provides a basis to integrate other frameworks, standards and practices as one single framework

Stakeholder Needs- what this is all about

Enterprises exist to create value for their stakeholders. Consequently, any enterprise- commercial or not-will have value creation as a governance objective. Value creation means realizing benefits at an optimal resource cost while optimizing risk:



Benefits can take many forms, e.g. financial for commercial enterprises or public service for government entities.

Enterprises have many stakeholders, and 'creating value' means different—and sometimes conflicting—things to each of them. Governance is about negotiating and deciding amongst different stakeholders' value interests. By consequence, the governance system should consider all stakeholders when making benefit, risk and resource assessment decisions For each decision, the following questions can and should be asked For whom are the benefits? Who bears the risk? What resources are required?

COBIT 5 Goals Cascade

Every enterprise operates in a different context: this context is determined by external factors (the market, the industry, geopolitics, etc.) and internal factors (the culture, organisation, risk appetite, etc.), and requires a customised governance and management system.

Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customised enterprise goals, IT-related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

The COBIT 5 goals cascade is shown here:

COBIT translates **stakeholder needs** into specific, actionable enterprise goals that cascade to IT-related goals then to specific enabler (i.e., processes) goals and practices.

This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

Step 1. Stakeholder Drivers Influence Stakeholder Needs

Stakeholder needs are influenced by a number of drivers, e.g., strategy changes, a changing business and regulatory environment, and new technologies.

Step 2 Stakeholder Needs Cascade to Enterprise Goals

Stakeholder needs can be related to a set of generic enterprise goals. These enterprise goals have been developed using the balanced scorecard (BSC), dimensions, and they represent a list of commonly used goals that an enterprise may define for itself. Although this list is not exhaustive, most enterprise-specific goals can be mapped easily onto one or more of the generic enterprise goals. Below are tables of stakeholder needs and enterprise goals.

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

COBIT 5 defines 17 generic goals, as shown above, which includes the following information:

- The Balanced Scorecard dimension under which the enterprise goal fits
- Enterprise goals
- The relationship to the three main governance objectives—benefits realisation, risk optimisation and resource optimisation. ('P' stands for primary relationship and “S” for secondary relationship, i.e., a less strong relationship.)

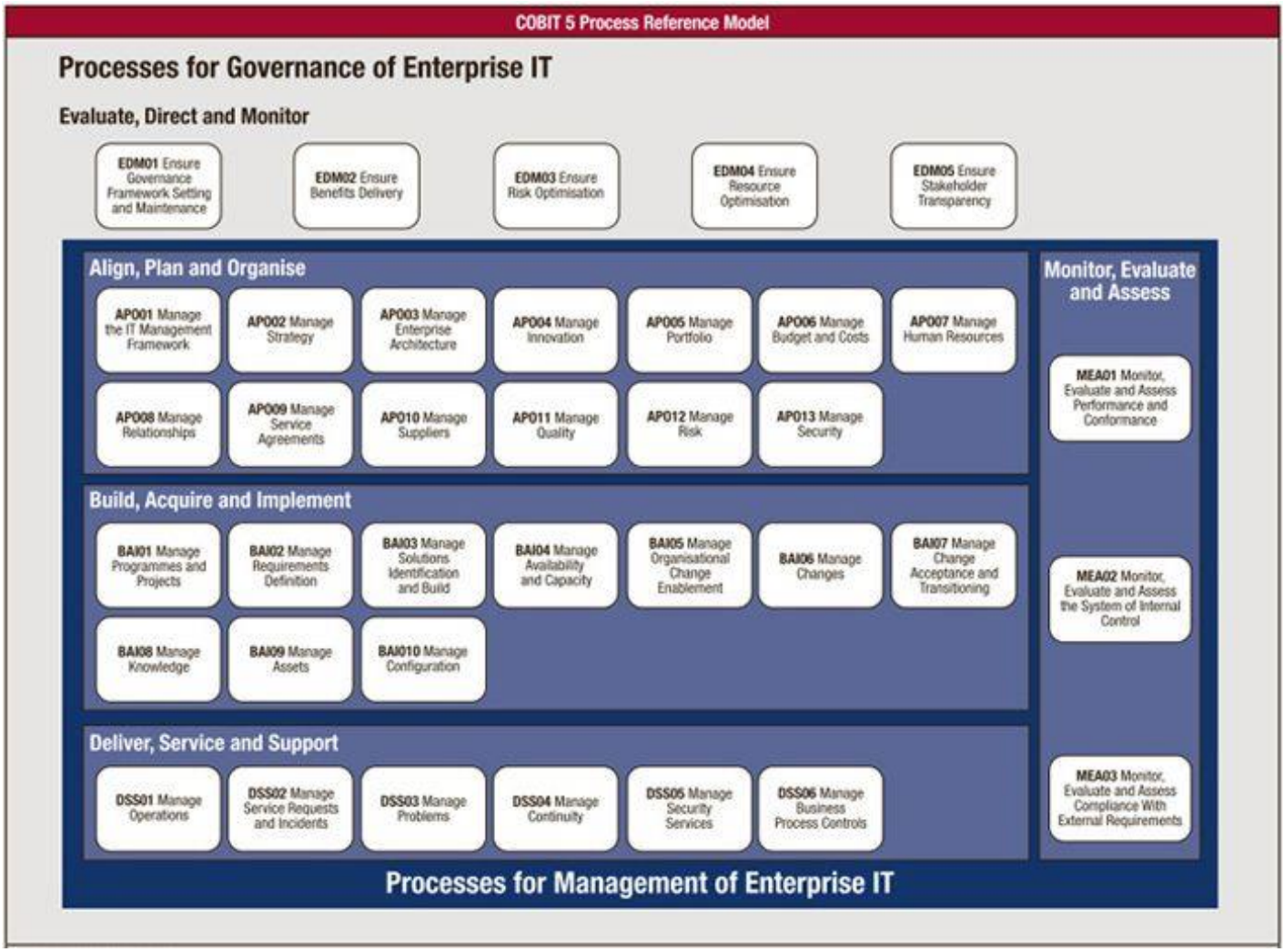
Step 3. Enterprise Goals Cascade to IT-related Goals

Achievement of enterprise goals requires a number of IT-related outcomes, which are represented by the IT-related goals. IT-related stands for information and related technology, and the IT-related goals are structured along the dimensions of the IT balanced scorecard (IT BSC). COBIT 5 defines 17 IT-related goals, listed below:

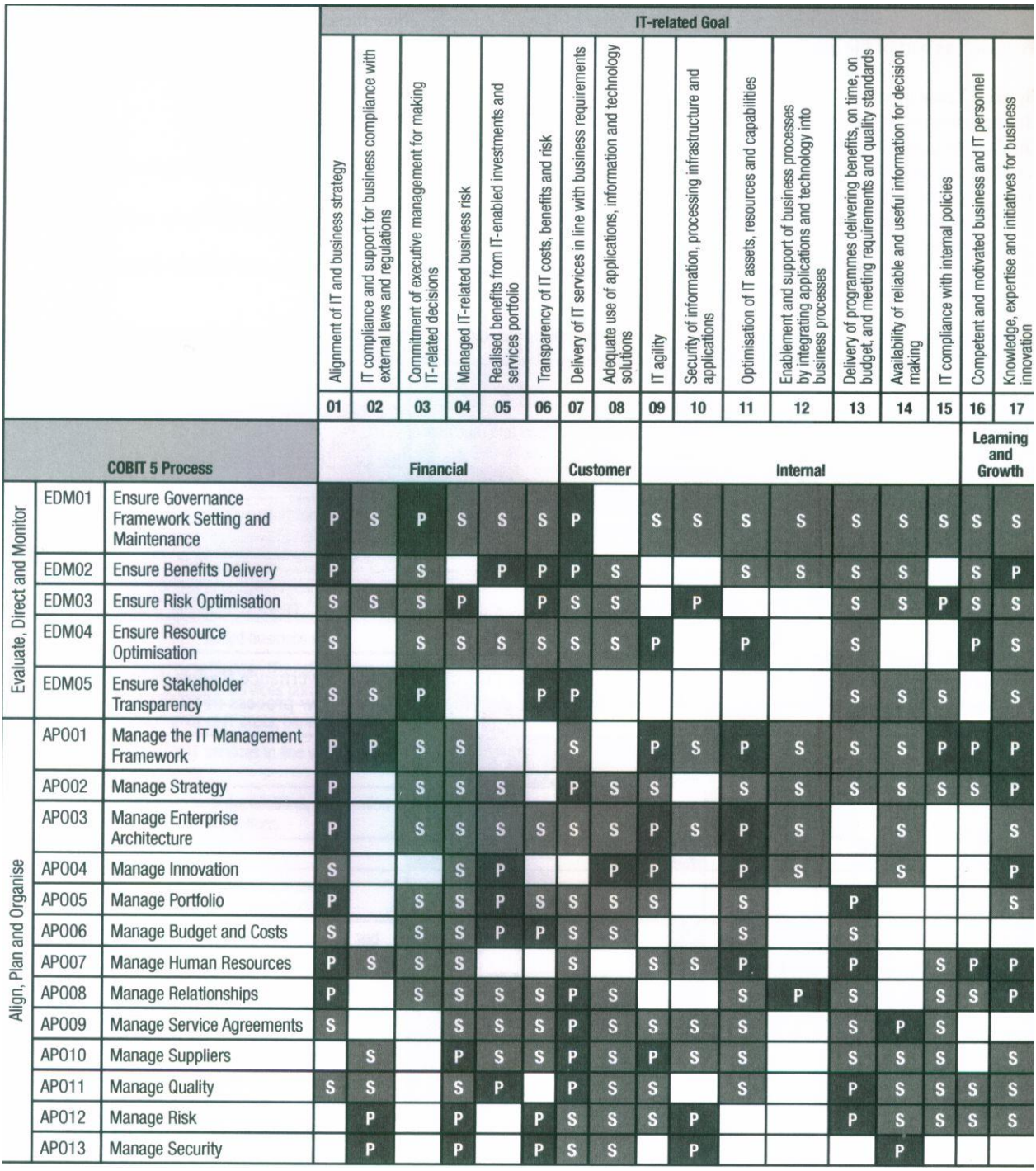
IT BSC Dimension	Information and Related Technology Goal	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

Step 4. IT-related Goals Cascade to Enabler Goals

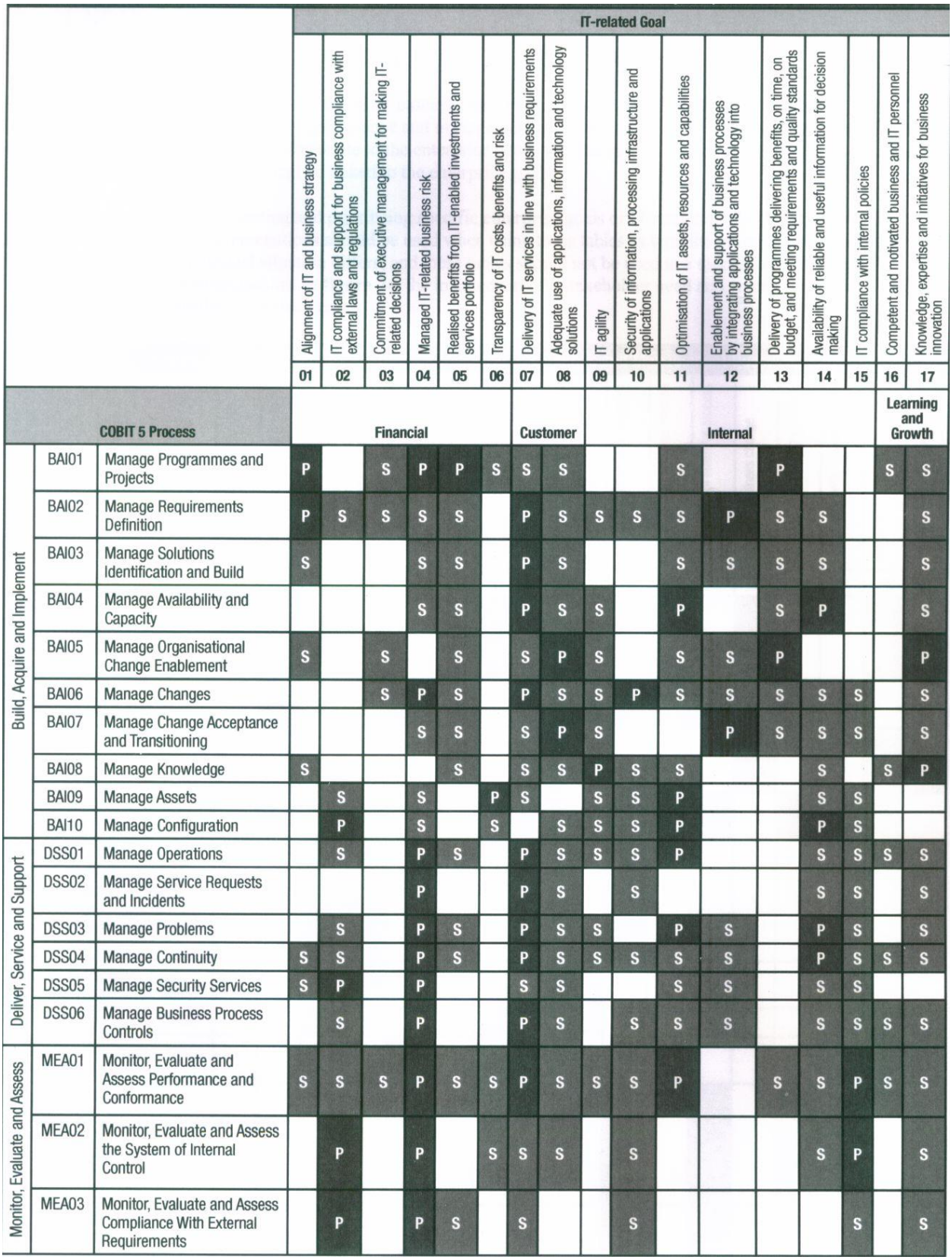
Achieving IT-related goals requires the successful application and use of a number of enablers. Enablers include processes, organisational structures and information, and for each enabler a set of specific relevant goals can be defined in support of the IT-related goals. The goals fall into the two categories of governance (grey background) and management (blue background):



Processes are one of the enablers, and appendix C contains a mapping between IT-related goals and the relevant COBIT 5 processes, which then contain related process goals. A condensed version of the linkage is shown here:



			IT-related Goal																
			Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risk	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	COBIT 5 Process		Financial						Customer		Internal							Learning and Growth	
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Ensure Benefits Delivery	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Ensure Risk Optimisation	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Ensure Resource Optimisation	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Ensure Stakeholder Transparency	S	S	P			P	P						S	S	S		S
Align, Plan and Organise	AP001	Manage the IT Management Framework	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	AP002	Manage Strategy	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	AP003	Manage Enterprise Architecture	P		S	S	S	S	S	S	P	S	P	S		S			S
	AP004	Manage Innovation	S			S	P			P	P		P	S		S			P
	AP005	Manage Portfolio	P		S	S	P	S	S	S	S		S		P				S
	AP006	Manage Budget and Costs	S		S	S	P	P	S	S			S		S				
	AP007	Manage Human Resources	P	S	S	S			S		S	S	P		P		S	P	P
	AP008	Manage Relationships	P		S	S	S	S	P	S			S	P	S		S	S	P
	AP009	Manage Service Agreements	S			S	S	S	P	S	S	S	S		S	P	S		
	AP010	Manage Suppliers		S		P	S	S	P	S	P	S	S		S	S	S		S
	AP011	Manage Quality	S	S		S	P		P	S	S		S		P	S	S	S	S
	AP012	Manage Risk		P		P		P	S	S	S	P			P	S	S	S	S
	AP013	Manage Security		P		P		P	S	S		P				P			



			IT-related Goal																
			Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risk	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	COBIT 5 Process		Financial						Customer		Internal							Learning and Growth	
Build, Acquire and Implement	BAI01	Manage Programmes and Projects	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Manage Requirements Definition	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Manage Solutions Identification and Build	S			S	S		P	S			S	S	S	S			S
	BAI04	Manage Availability and Capacity				S	S		P	S	S		P		S	P			S
	BAI05	Manage Organisational Change Enablement	S		S		S		S	P	S		S	S	P				P
	BAI06	Manage Changes			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Manage Change Acceptance and Transitioning				S	S		S	P	S			P	S	S	S		S
	BAI08	Manage Knowledge	S				S		S	S	P	S	S			S		S	P
	BAI09	Manage Assets		S		S		P	S		S	S	P			S	S		
	BAI10	Manage Configuration		P		S		S		S	S	S	P			P	S		
Deliver, Service and Support	DSS01	Manage Operations		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Manage Service Requests and Incidents				P			P	S		S				S	S		S
	DSS03	Manage Problems		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Manage Continuity	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Manage Security Services	S	P		P			S	S			S	S		S	S		
	DSS06	Manage Business Process Controls		S		P			P	S		S	S	S		S	S	S	S
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Monitor, Evaluate and Assess the System of Internal Control		P		P		S	S	S		S				S	P		S
	MEA03	Monitor, Evaluate and Assess Compliance With External Requirements		P		P	S		S			S					S		S

Once again, “P” represents a primary relationship and “S” a secondary one.

Benefits of the COBIT 5 Goals Cascade

The goals cascade is important because it allows the definition of priorities for implementation, improvement and assurance of governance of enterprise IT based on (strategic) objectives of the enterprise and the related risk. In practice, the goals cascade:

- Defines relevant and tangible goals and objectives at various levels of responsibility
- Filters the knowledge base of COBIT 5, based on enterprise goals, to extract relevant guidance for inclusion in specific implementation, improvement or assurance projects
- Clearly identifies and communicates how (sometimes very operational) enablers are important to achieve enterprise goals

Using the COBIT 5 Goals Cascade Carefully

The goals cascade—with its mapping tables between enterprise goals and IT-related goals and between IT-related goals and COBIT 5 enablers (including processes)—does not contain the universal truth, a. users should not attempt to use it in a purely mechanistic way, but rather as a guideline. There are various reasons for this, including:

- Every enterprise has different priorities in its goals, and priorities may change over time.
- The mapping tables do not distinguish between size and/or industry of the enterprise. They represent a sort of common denominator of how, in general, the different levels of goals are interrelated.
- The indicators used in the mapping use two levels of importance or relevance, suggesting that there are 'discrete' levels of relevance, whereas, in reality, the mapping will be close to a continuum of various degrees of correspondence.

Using the COBIT 5 Goals Cascade in Practice

From the previous disclaimer, it's obvious that the first step an enterprise should always apply when using the goals cascade is to customise the mapping, taking into account its specific situation. In other words, each enterprise should build its own goals cascade, compare it with COBIT and then refine it.

For example, the enterprise may wish to:

- Translate the strategic priorities into a specific 'weight' or importance for each of the enterprise goals.
- Validate the mappings of the goals cascade, taking into account its specific environment, industry, etc.

Finally…

Below we see another view of stakeholder goals- the internal and external stakeholders and the IT-related questions that are relevant for each. Notice how they sound very much like a set of questions that this course aims to answer…

Internal Stakeholders	Internal Stakeholder Questions
• Board • Chief executive officer (CEO) • Chief financial officer (CFO) • Chief information officer (CIO) • Chief risk officer (CRO) • Business executives • Business process owners • Business managers • Risk managers • Security managers • Service managers • Human resource (HR) managers • Internal audit • Privacy officers • IT users • IT managers • Etc.	• How do I get value from the use of IT? Are end users satisfied with the quality of the IT service? • How do I manage performance of IT? • How can I best exploit new technology for new strategic opportunities? • How do I best build and structure my IT department? • How dependent am I on external providers? How well are IT outsourcing agreements being managed? How do I obtain assurance over external providers? • What are the (control) requirements for information? • Did I address all IT-related risk? • Am I running an efficient and resilient IT operation? • How do I control the cost of IT? How do I use IT resources in the most effective and efficient manner? What are the most effective and efficient sourcing options? • Do I have enough people for IT? How do I develop and maintain their skills, and how do I manage their performance? • How do I get assurance over IT? • Is the information I am processing well secured? • How do I improve business agility through a more flexible IT environment? • Do IT projects fail to deliver what they promised—and if so, why? Is IT standing in the way of executing the business strategy? • How critical is IT to sustaining the enterprise? What do I do if IT is not available? • What critical business processes are dependent on IT, and what are the requirements of business processes? • What has been the average overrun of the IT operational budgets? How often and how much do IT projects go over budget? • How much of the IT effort goes to fighting fires rather than to enabling business improvements? • Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives? • How long does it take to make major IT decisions? • Are the total IT effort and investments transparent? • Does IT support the enterprise in complying with regulations and service levels? How do I know whether I am compliant with all applicable regulations?

External Stakeholders	External Stakeholder Questions
• Business partners • Suppliers • Shareholders • Regulators/government • External users • Customers • Standardisation organisations • External auditors • Consultants • Etc.	• How do I know my business partner's operations are secure and reliable? • How do I know the enterprise is compliant with applicable rules and regulations? • How do I know the enterprise is maintaining an effective system of internal control? • Do business partners have the information chain between them under control?