COBIT 5 Framework

Saturday, 23 September, 2017 3:51 PM

COBIT 5:

- A business framework for the governance and management of Enterprise IT.

Enablers:

- Anything that can help to achieve the objectives of the enterprise.

Governance:

- Governance ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization 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 organizational structures at an appropriate level, particularly in larger, complex enterprises.

Management:

- 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 chief executive officer (CEO).

- Enterprise exist to create value for their stakeholder.
- Enterprises have many stakeholder.
- The governance system should consider all stakeholder when making benefits, risk and resource assessment decision.

Overview of This Publication:

- The COBIT 5 framework contains seven more chapters:
  - Chapter 2 elaborates on Principle 1, **Meeting stakeholders needs**.
    - It introduces the COBIT 5 goals cascade
    - The enterprise goals for IT are used to formalize and structure the stakeholder needs.
    - Enterprise goals can be linked to IT-related goals, and these IT-related goals can be achieved through optimal use and execution of all enablers, including processes
    - This set of connecting goals is called the COBIT 5 goal cascade.
  - Chapter 3 elaborates on principle 2, **Covering the Enterprise End-to-end**
    - It explains how COBIT5 integrates governance of enterprise IT into enterprise governance by covering all functions and processes within the enterprise.
  - Chapter 4 elaborates on principle 3, **Applying Single Integrated Framework,** and describes briefly the COBIT 5 architecture that achieves the integration.
  - Chapter 5 elaborates on principle 4, **Enabling a Holistic Approach**.
    - Governance of enterprise IT is systemic and supported by a set of enablers. In this chapter, enablers are introduced and a common way of looking at enablers is presented: the generic enabler model.
  - Chapter 6 elaborates on principle 5, **Separating Governance from Management**, and discuss the difference between management and governance, and how they interrelate. The high-level COBIT 5 process reference model is included as an example.
  - Chapter 7 contains an introduction to **Implementation Guidance.**
    - It describes how the appropriate environment can be created, the enablers required, typical pain points and trigger events for implementation and continual improvement life cycle.
    - This chapter is based on the publication title COBIT 5 Implementation, where full details on how to implement governance of Enterprise IT based on COBIT 5 can be found.
  - Chapter 8 elaborates on **The COBIT 5 Process Capability Model** in the COBIT assessment program approach scheme, how it differs from **COBIT 4.1 process maturity assessments**, and how users can migrate to the new approach.

- **COBIT 5 Goal Cascade:**
  - Every enterprise operates in different context; this context is determine by external factors (the market, the industry, geopolitical, etc.) and internal factors (the culture, organization, risk appetite, etc.), and requires a customized governance and management system.
  - Stakeholder needs have to be transformed into an enterprise's actionable strategy.

- **Benefits of Goal 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 goal cascade:
    - Defines relevant and tangible goals and objectives at various levels of responsibilities
    - Filter the knowledge base of COBIT5, based on enterprise goals, to extract relevant guidance for inclusion in specific implementation, improvement or assurance projects.
    - Clearly identifies and communicates how (sometime very operational) enables are important to

- ITIL - Information Technology Infrastructure Library
- TOGAF - The Open Group Architecture Forum
- PMBOK - Project Management Body of Knowledge
- PRINCE2- PRoject IN Controlled Environments 2
- COSO - Committee of Sponsoring Organizations of the Tredway Commission
- BMIS - Business Model for Information Security
- ITAF - IT Assurance Framework
- ISO/IEC 38500:2008 - Corporate Governance of Information Technology

A **process** is defined as a collection of practices influenced by the enterprise's policies and procedures that takes inputs form a number of sources (Including other processes), manipulates the inputs and produces outputs (e.g., products, services) '

The enabler goals are the final step in the COBIT 5 goal cascade. Goal can be further split into different categories:

- **Intrinsic Quality:**
  - The extent to which enabler works accurately, objectively and provide accurate, objective and reputable result.
- **Contextual Quality**
  - The extent to which enablers and their outcomes are fit for purpose given the context in which they operate. E.g., outcomes should be relevant, complete, current, and appropriate, consistent, understandable and easy to use.
- **Access and Security**
  - The extent to which enablers and their outcomes are accessible and secured. Such as:
    - Enablers are available when, and if needed.
    - Outcomes are secured, i.e., if access is restricted to those entitled and needing it.
- **Life Cycle**
  - Each enabler has a life cycle, from inception through an operational/useful life cycle disposal. This applies to information, structures, processes, policies, etc. The phase of life cycle consist of:
    - Plan (includes concepts development and concepts selection)
    - Design
    - Build/acquire/create/implement
    - Use/Operate
    - Evaluate/Monitor
    - Update/dispose
- **Good practices**
  - For each of the enablers, good practices can be defined. Good practices support the achievement of the enablers goals. Good practices provide examples or suggestions on how best to implement the enabler, and what work products or inputs and outputs are required. COBIT 5 Provides examples of good practices for some enablers, guidance from other standards, frameworks, etc., can be used.

achieve enterprise goals.

- **Using the COBIT 5 goals cascade carefully**
  - The goals cascade -- with its mapping tables enterprise enterprise goals and IT-Related goals and between IT related goals and COBIT 5 enablers (including process) - does not contain universal truth, and user should not attempt to use it in a purely mechanistic way, but rather as a guideline. There are various reason for this including:
    - Every enterprise has different priorities in its goals, and prioritize may change over time.
    - The mapping table 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 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 minimum of various degree of correspondence
- **Governance Enablers:**
  - Governance enablers are the organizational resources for governance, such as frameworks, principles, structures, processes and practices, through or towards which action is directed and objective can be attained.
  - Enablers also include the resource enterprise's resource - e.g. service capabilities (IT infrastructure, applications etc.), people and information
  - A lack of resource or enablers may affect the ability of the enterprise to create value.

Enablers:

- Enablers are factors that, individually and collectively, influences whether something will work - in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e. higher-level IT-related goals define what the different enablers should achieve.
- COBIT 5 framework describes seven categories of enablers:
  - **Principles, policies, and framework** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
  - **Process** describes an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
  - **Organizational structure** are key decision making entities in an enterprise.
  - **Culture, ethics and behavior** of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
  - **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, operation is very often the key product of the enterprise itself.
  - **Service, infrastructure and applications** include the infrastructure, technology and applications that provide enterprise with information technology processing and services.
  - **People, skills and competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

COBIT5 Enabler Dimensions:

- All enablers have a set of common dimensions. This set of common dimensions:
  - Provide a common, simple and structured way to deal with enablers
  - Allows an entity to manage its complex interactions
  - Facilitates successful outcomes of the enablers
- **Enabler Dimensions**
  - The four common dimensions for enablers are:
    - **Stakeholders**
      - Internal Stakeholders
      - External Stakeholders
    - **Goals**
      - Each enablers has a number of goals, and enablers provide value by the achievement of these goals. Goals can be defined in term of:
        - Expected outcomes of the enablers
        - Application or operation of the enabler itself
      - The enabler goals are the final step in the COBIT 5 goal cascade. Goals can be further split up in different categories.

- **Interaction between Governance and Management**
  - From the governance and management, it is clear that they comprise different types of activities, with different responsibilities; however, given the role of governance - to evaluate, direct and monitor - a set of interactions is required between governance and management to result in an efficient and effective governance system.

- **Implementation Guidance:**
  - Optimal value can be realized from leveraging COBIT only if it is effectively adopted and adapted to suit each enterprise's unique environment. Each implementation approach will also need to address specific challenges, including managing changes to culture and behavior.
  - ISACA provides practical and extensive implementation guidance in its publication COBIT 5 implementation, which is based on a continual improvement life cycle. It is not intended to be a prescriptive approach nor a complete solution, but rather a guide to avoid commonly encountered pitfalls, leverage good practices and assist in the creation of successful outcomes.

- **Key success factors for successful implementation include:**
  - Top management providing the direction and mandate for the initiative, as well as visible ongoing commitment and support.
  - All parties supporting the governance and management processes to understand the business and IT objectives.
  - Ensuring effective communication and enablement of the necessary changes.
  - Tailoring COBIT and other supporting good practices and standards to fit the unique context of the

enterprise.
    - Focusing on quick wins and prioritizing the most beneficial improvements that are easiest to implement.

- **Recognizing Pain points and trigger events**
    - There are a number of factors that may indicate a need for improvement governance and management of enterprise IT.
    - By using pain points or trigger events as the launching point for implementation initiatives, the business case for governance and management of enterprise IT improvement can be related to practical, everyday issues being experienced.
    - This will improve buy-in and create the sense of urgency within enterprise that is necessary to kick off the implementation.

    - Examples of some the typical pain points for which new or revised governance or management of IT enablers can be a solution (or part of a solution), as identified in COBIT 5 Implementation, are:
        - Business frustration with failed initiatives, rising IT costs and a perception of low business value.
        - Significant incidents related to IT risk, such as data loss or project failure.
        - Outsourcing service delivery problems, such as consistent failure to meet agreed-on service levels
        - Failure to meet regulatory or contractual requirements
        - IT limiting the enterprise's innovation capability and business agility
        - Regular audit findings about poor IT performance or reported IT quality of service problems
        - Hidden and rouge IT spending
        - Complex IT operating models

    - In addition to these pain points, other events in the enterprise's internal and external environments can signal or trigger a focus on the governance and management of IT. Examples from chapter 3 in the COBIT 5 implementation publication are:
        - Merger, acquisition, or divestiture.
        - A shift in the market, economy or competitive positions
        - A change in the business operating model or sourcing arrangements
        - New regulatory or compliance requirements
        - A significant technology change or paradigm shift
        - An enterprise wide governance focus or projects
        - A new CEO, CFO, CIO etc.
        - External audit or consultant assessments
        - A new business strategy or priority

- **Enabling Changes**
    - Successful implementation depends on implementing the appropriate changes (the appropriate governance or management enablers) in the appropriate way. In many enterprise, there is a significant focus on the first aspect - core governance or management of IT - but not enough emphasis on managing the human, behavioral and cultural aspects of the changes and motivating stakeholders to buy into the change.

- **A Life Cycle Approach**
    - The implementation life cycle provides a way for enterprise to use COBIT to address the complexity and challenges typically encountered during implementation. The interrelated components of the life cycle are the:
        - Core continual improvement life cycle - This is not a one-off project.
        - Enablement of change - Addressing the behavioral and cultural aspects.
        - Management of the program.

- **The seven phases of the implementation life cycle**
    - Program management
        - Outer ring
    - Change enablement
        - Middle ring
    - Continual improvement life cycle
        - Inner ring
- **Phase 1:** Starts with recognizing and agreeing to the need for an implementation or improvement initiatives. It identifies the current pain points and triggers and creates a desire to change at executive management levels.

- **Phase 2:** is focused on defining the scope of the implementation or improvement initiative using COBIT's mapping of enterprise goals to IT-related goals to the associated IT process, and consideration how risk scenarios could also highlight key process on which to focus. High-level diagnostics can also be useful for scoping and understanding high priority areas on which to focus. An assessment of the current state is then performed, and issues or deficiencies are identified by carrying out a process capability assessment. Large-scale initiatives should be structured as multiple iterations of the life cycle -- for any implementation initiative exceeding six months there is a risk of losing momentum, focus and buy-in from stakeholders.

- During **phase 4** plans practical solutions by defining projects supported by justifiable business cases. A change plan for implementation is also developed. A well-developed business case helps to ensure that the project's benefits are identified and monitored.

- The propose solutions are implemented into day-to-day practices in **phase 5.** Measures can defined and monitoring established, using COBIT's goals metrics to ensure that business alignment is achieved and maintained and performance can be measured. Success requires the engagement and demonstrated commitment pf top management as well ownership by the affected business and IT stakeholders.

- **Phase 6** focuses on the sustainable operations of the new or improved enablers and the monitoring of the achievement of expected benefits.

- During **phase 7**, the overall success of the initiative is reviewed, further the requirement for the governance or management of the enterprise IT are identified, and the need for the continual improvement is reinforced.

The COBIT 5 process capability Model:

- Users of COBIT 4.1, Risk IT, and Val IT are familiar with the process maturity models included in those frameworks. These models are used to measure current 'as-is' maturity of an enterprise's IT-related processes, to define a required 'to-be' state of maturity, and to determine the gap between them and how to improve the process to achieve the desired maturity level.
- The COBIT 5 product set includes a process capability model, based on the internationally recognized ISO/IEC 15504 software engineering - Process Assessment Standard.
- This model will achieve the same overall objectives of the process assessment and process improvement support, i.e. it will provide a means to measure performance of any of the governance (EDM-based) processes or management (PBRM-based) processes, and will allow areas for improvement to be identified.
- However, the new model is different from COBIT 4.1 maturity model in its design and use, and for that reason, the following topics are discussed:
    - Differences between the COBIT 5 and COBIT 4.1 models
    - Benefits of COBIT 5 Model
    - Summary of the differences that COBIT 5 user will encounter in practice
    - Performing a COBIT 5 capability assessment

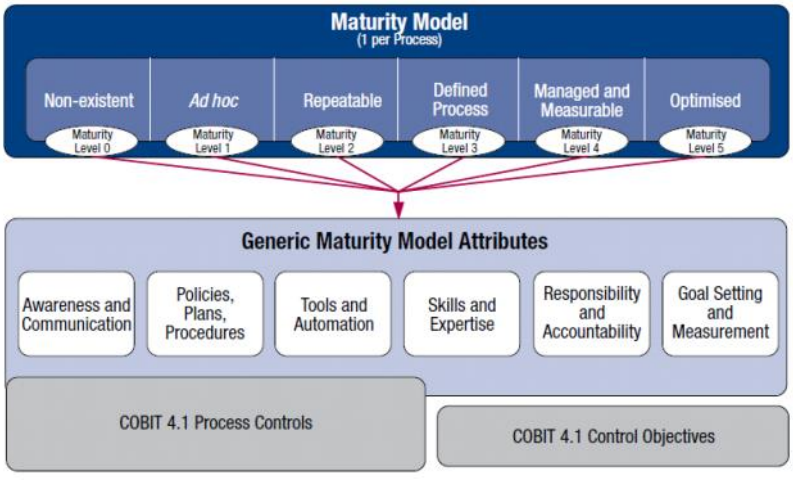
Difference Between the COBIT 4.1 maturity model and the COBIT 5 Process capability model

Maturity Model (1 per process)

- Maturity level 0
    - Non-existent
- Maturity level 1
    - Ad hoc
- Maturity level 2
    - Repeatable
- Maturity level 3
    - Defined process
- Maturity level 4
    - Managed and measureable
- Maturity level 5
    - Optimized

Generic Maturity Model Attributes:

- Awareness and communication
- Policies, plans and procedure
- Tools and automation
- Skills and expertise
- Responsibility and accountability
- Goal setting and measurement
- COBIT 4.1 Process controls
- COBIT 4.1 Control Objectives



Using the COBIT 4.1 maturity model for process improvement purposes -- assessing a process maturity, defining a target maturity level and identifying gaps - Required using the following COBIT 4.1 Components:

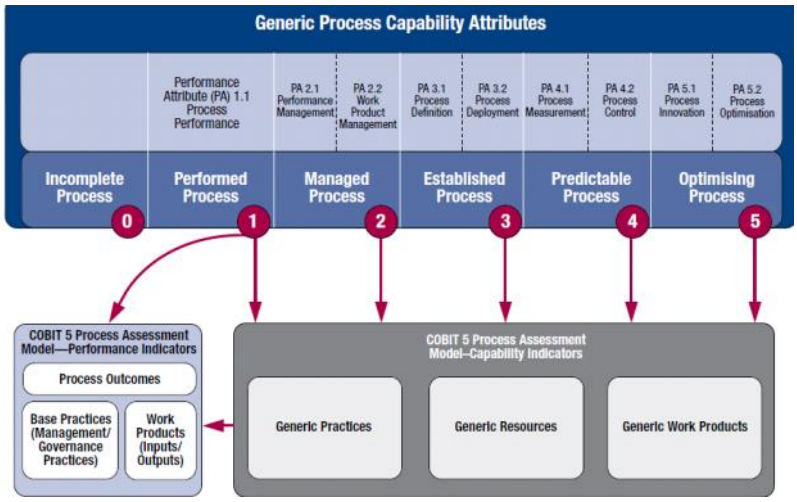
- First, an assessment needed to be made whether control objectives for the process were met.
- Next, the maturity model included in the management guidelines for each process could be used to obtain a maturity profile of the process.
- In addition, the generic maturity model in COBIT 4.1 provided six distinct attributes that were applicable for each process and that assisted in obtaining more detailed view on the process maturity level.
- Process controls are generic control objectives -- they also needed to be reviewed when a process assessment was made. Process controls partially overlap with the generic maturity model attributes.

The most important difference between an ISO/IEC 15504-based process capability assessment and the current COBIT 4.1 maturity model can be summarized as follow:

- The naming and meaning of the ISO/IEC 15504 defined capability levels are quite different from the current 4.1 maturity levels for processes.
- In ISO/IEC 15504, capability levels are define by a set of nine process attributes. These attributes cover some

ground covered by the current COBIT 4.1 maturity attributes and/or process controls, but only a certain extent
- and in a different way.

The COBIT 5 Process Capability Approach:



Comparison Table of Maturity Levels (COBIT 4.1) and Process Capability Levels (COBIT5)

COBIT 4.1 Maturity Model Level	Process Capability Based on ISO/IEC 15504	Context
5 Optimised—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.	**Level 5: Optimising process**—The level 4 predictable process is continuously improved to meet relevant current and projected business goals.	**Enterprise View—Corporate Knowledge**
4 Managed and measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.	**Level 4: Predictable process**—The level 3 established process now operates within defined limits to achieve its process outcomes.	
3 Defined process—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalisation of existing practices.	**Level 3: Established process**—The level 2 managed process is now implemented using a defined process that is capable of achieving its process outcomes.	
	Level 2: Managed process—The level 1 performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.	**Instance View—Individual Knowledge**
2 Repeatable but intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.	**Level 1: Performed process**—The implemented process achieves its process purpose. **Remark: It is possible that some classified as Maturity Model 1 will be classified as 15504 0, if the process outcomes are not achieved.**	
1 Initial/*Ad hoc*—There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.		
0 Non-existent—Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.	**Level 0: Incomplete process**—The process is not implemented or fails to achieve its purpose.	

Mapping of COBIT 5 with the most relevant related standard and frameworks:
- ISO/IEC 38500 Principles
  - Principle 1 - Responsibility
    - What this means in practice:
      - The business (customer) and IT (provider) should collaborate in a partnership model utilizing effective communications based on a positive and trusted relationship and demonstrating clarity regarding responsibility and accountability. For larger enterprises, an IT executive committee (also referred to as the IT strategy committee) acting on behalf of the board and chaired by a board member is a very effective mechanism for evaluating, directing and monitoring the use of

IT in the enterprise and for advising the board on critical IT issues. Directors of small and medium -sized enterprises with a simpler command structure and shorter communication paths need to take a more direct approach when overseeing IT activities. In all cases, appropriate governance organizational structures, roles and responsibilities are required to be mandated from the governing body, providing clear ownership and accountability for important decisions and tasks. This should include relationships with key third-party IT service providers.

- How ISACA's guidance enables good practice:
  1) The COBIT 5 framework defines a number of enablers for governance of enterprise IT. The 'process' enabler and the 'organizational structures' enabler, combined with the RACI13 charts, are particularly relevant in this context. They strongly advocate assignment of responsibilities, and provide example roles and responsibilities for board members and management for all key related processes and activities.
  2) COBIT 5 Implementation explains the responsibilities of stakeholders and other involved parties when implementing or enhancing IT governance arrangements.
  3) COBIT 5 has two levels of monitoring. The first level is relevant in a governance context. The process EDM05 Ensure stakeholder transparency explains the director's role in monitoring and evaluating IT governance and IT performance with a generic method for establishing goals and objectives and related metrics.

- Principle 2—Strategy
  - What this means in practice:
    - IT strategic planning is a complex and critical undertaking requiring close co -ordination amongst enterprise wide business unit and IT strategic plans. It is also vital to priorities the plans most likely to achieve the desired benefits an d to allocate resources effectively. High-level goals need to be translated into achievable tactical plans, ensuring minimal failures and surprises. The goal is to deliver value in support of strategic objectives while considering the associated risk in relation to the board's risk appetite. While it is important to cascade plans in a top -down fashion, the plans must also be flexible and adaptable to meet rapidly changing business requirements and IT opportunities.

    - Furthermore, the presence or absence of IT capabilities can either enable or hinder business strategies; therefore, IT strategic planning should include transparent and appropriate planning of IT capabilities. This should include assessment of the ability of the current IT infrastructure and human resources to support future business requirements and consideration of future technological developments that might enable competitive advantage and/or optimize costs. IT resources include relationships with many external product vendors and service providers, some of whom likely play a critical role in supporting the business. Governance of strategic sourcing is thus a very significant strategic planning activity requiring executive-level direction and oversight.
  - How ISACA's guidance enables good practice:
    1) COBIT 5 provides specific guidance on managing IT investments and (specifically, in the process EDM02 Ensure benefits delivery in the governance domain) how strategic objectives should be supported by appropriate business cases.

    2) The COBIT 5 APO domain explains the processes required for the effective planning and organization of internal and external IT resources, including strategic planning, technology and architecture planning, organizational planning, innovation planning, portfolio management, investment management, risk management, relationship management and quality management. The alignment of business and IT goals is also explained, with generic examples showing how they support strategic objectives for all IT-related processes based on industrywide research.

    3) The exercise of identifying and aligning enterprise goals and IT -related goals presents a better understanding of the cascading relationship amongst enterprise goals, IT-related goals and enablers, which include IT processes. It presents a solid and strong list of 17 generic enterprise goals and 17 generic IT -related goals, validated and prioritized amongst different sectors. Together with the linking information between both, it provides a good basis on which to build a generic cascade from business goals to IT goals.

- Principle 3—Acquisition
  - What this means in practice:
    - IT solutions exist to support business processes and therefore care must be taken to not consider IT solutions in isolation or as just a 'technology' project or service. On the other hand, an inappropriate choice of technology architecture, a failure to maintain a current and appropriate technical infrastructure, or an absence of skilled human resources can result in project failure, an inability to sustain business operations or a reduction in value to the business. Acquisitions of IT resources should be considered as a part of wider IT -enabled business change. The acquired technology must also support and operate with existing and planned business processes and IT infrastructures. Implementation is also not just a technology issue, but rather a combination of organizational change, revised business processes, training and enabling the change. Therefore, IT projects should be undertaken as part of wider enterprise wide change programmers that include other projects satisfying the full range of activities required to help ensure a successful outcome.

  - How ISACA's guidance enables good practice:
    1) The COBIT 5 EDM domain provides guidance on governing and managing IT -enabled business investments through their complete life cycle (acquisition, implementation, operation and decommissioning). The APO05 Manage portfolio process addresses how to apply effective portfolio and programme management of such investments to help ensure that benefits are realized and costs are optimized.
    2) The COBIT 5 APO domain provides guidance for planning for acquisition, including investment planning, risk management, programme and project planning, and quality planning.
    3) The COBIT 5 BAI domain provides guidance on the processes required to acquire and implement IT solutions, covering defining requirements, identifying feasible solutions, preparing documentation, and training and enabling users and operations to run the new systems. In addition, guidance is provided to help ensure that the solutions are tested and controlled properly as the change is applied to the operational business and IT environment.
    4) The COBIT 5 MEA domain and process EDM05 include guidance on how directors can monitor and evaluate the acquisition process, and internal controls to help ensure that acquisitions are properly managed and executed.

- Principle 4—Performance
  - What this means in practice:
    - Effective performance measurement depends on two key aspects being addressed: the clear definition of performance goals and the establishment of effective metrics to monitor achievement of goals. A performance measurement process is also required to help ensure that performance is monitored consistently and reliably. Effective governance is achieved when goals are set from the top down and aligned with high -level, approved business goals, and metrics are established from the bottom up and aligned in a way that enables the achievement of goals at all levels to be monitored by each layer of management. Two critical governance success factors are the approval of goals by stakeholders, and the acceptance of accountability for achievement of goals by directors and managers. IT is a complex and technical topic;

therefore, it is important to achieve transparency by expressing goals, metrics and performance reports in language meaningful to the stakeholders so that appropriate actions can be taken.

- How ISACA's guidance enables good practice:
  1) The COBIT 5 framework provides generic examples of goals and metrics for the full range of IT -related processes and the other enablers, and shows how they relate to business goals, enabling enterprises to adapt them for their own specific use.
  2) COBIT 5 provides management with guidance on setting IT objectives in alignment with business goals and describes how to monitor performance of these objectives using goals and metrics. Process capability can be assessed using an ISO/IEC 15504 compliance capability assessment model.
  3) Two key COBIT 5 processes provide specific guidance:
     - APO02 Manage strategy focusses on setting goals.
     - APO09 Manage service agreements focusses on defining appropriate services and service goals and documenting them in service level agreements.
  4) In process MEA01 Monitor, evaluate and assess performance and conformance, COBIT 5 provides guidance on responsibilities of executive management for this activity.
  5) The planned COBIT 5 for Assurance guide will explain how assurance professionals can provide independent assurance to directors regarding IT performance.

- Principle 5—Conformance
  - What this means in practice:
    - In today's global marketplace, enabled by the Internet and advanced technologies, enterprises need to comply with a growing number of legal and regulatory requirements. Because of corporate scandals and financial failures in recent years, there is a heightened awareness in the boardroom of the existence and implications of tougher laws and regulations. Stakeholders require increased assurance that enterprises are complying with laws and regulations and conforming to good corporate governance practice in their operating environment. In addition, because IT has enabled seamless business processes between enterprises, there is also a growing need to help ensure that contracts include important IT-related requirements in areas such as privacy, confidentiality, intellectual property and security.

      Directors need to ensure that compliance with external requirements is dealt with as a part of strategic planning rather than as a costly afterthought. They also need to set the tone at the top and establish policies and procedures for their management and staff to follow, to ensure that the goals of the enterprise are realized, risk is minimized and compliance is achieved. Top management must strike an appropriate balance between performance and conformance, ensuring that performance goals do not jeopardize compliance and, conversely, that the conformance regime is appropriate and does not overly restrict the operation of the business.

  - How ISACA's guidance enables good practice:
    1) The COBIT 5 governance and management practices provide a basis for establishing an appropriate control environment in the enterprise. The process capability assessments enable management to evaluate and benchmark IT process capability.
    2) COBIT 5 process APO02 Manage strategy helps ensure that there is alignment between the IT plan and the overall business objectives, including governance requirements.
       COBIT 5 process MEA02 Monitor, evaluate and assess the system of internal control enables directors to assess whether controls are adequate to meet compliance requirements.
    3) COBIT 5 process MEA03 Monitor, evaluate and assess compliance with external requirements helps ensure that external compliance requirements are identified, directors set the direction for compliance, and IT compliance itself is monitored, assessed and reported as a part of overall conformance to enterprise requirements.
    4) The planned COBIT 5 for Assurance guide explains how auditors can provide independent assurance of compliance and adherence to internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner.

- Principle 6—Human Behavior
  - What this means in practice:
    - The implementation of any IT-enabled change, including IT governance itself, usually requires significant cultural and behavioral change within enterprises as well as with customers and business partners. This can create fear and misunderstanding amongst staff, so implementation needs to be managed carefully if personnel are to remain positively engaged. Directors must clearly communicate goals and be seen as positively supporting the proposed changes. Training and skills enhancement of personnel are key aspects of change —especially given the rapidly moving nature of technology. People are affected by IT at all levels in an enterprise, as stakeholders, managers and users, or as specialists providing IT-related services and solutions to the business. Beyond the enterprise, IT affects customers and business partners and increasingly enables self-service and automated intercompany transactions within countries and across borders. While IT-enabled business processes bring new benefits and opportunities, they also carry increasing types of risk. Issues such as privacy and fraud are growing concerns for individuals, and these and other types of risk need to be managed if people are to trust the IT systems they use. Information systems can also dramatically affect working practices by automating manual procedures.
  - How ISACA's guidance enables good practice:
    - The following COBIT 5 enablers (which include processes) provide guidance on requirements relating to human behavior:
      - COBIT 5 enablers include people, skills and competencies, and culture, ethics and behavior. For each enabler a model is presented on how to deal with the enabler, illustrated by examples.
      - COBIT 5 process APO07 Manage human resources explains how the performance of individuals should be aligned with corporate goals, how IT specialist skills should be maintained, and how roles and responsibilities should be defined.
      - COBIT 5 process BAI02 Manage requirements definition helps ensure design of applications to meet human operation and use requirements.
      - COBIT 5 processes BAI05 Manage organizational change enablement and BAI08 Manage knowledge help ensure that users are enabled to use systems effectively.