Foundation Workshop

Dr. Pratul Sharma

ITIL Expert, PRINCE2, PMP,

Certified Scrum Master, Six Sigma

Chief Mentor Vedang Software

www.vedangsoftware.com

COBIT 5:
A Business Framework for the Governance and Management of Enterprise IT

Purpose

To confirm that a candidate has sufficient knowledge and understanding of the COBIT 5 Guidance and Management of enterprise IT, create awareness with their business executives and senior IT Management ; assess the current state of their Enterprise IT with the objective of scoping what aspects of COBIT 5 would be appropriate to implement.

The Foundation level training and certificate is also a prerequisite for the following training and certificate courses

- COBIT 5 Implementation Training & Certificate
- COBIT 5Assessor Training & Certificate

Target Audience

- Business Management
- Chief Executives
- IT/IS Auditors
- Information Security and IT Practitioners
- Consultants
- IT/IS Management
  - Looking to gain an insight into the Enterprise Governance of ITand looking to be certified as a COBIT Implementer or Assessor

High Level Learning Outcomes

The candidate should understand the key principles and terminology within COBIT 5. Specifically the candidate should know and understand :

- The major drivers for the development of a Framework.
- The business benefits of using COBIT 5.
- The COBIT 5 ProductArchitecture.
- The IT management issues and challenges that affect enterprises.
- The 5 Key Principles of COBIT 5 for the governance and management of Enterprise IT
- How COBIT 5 enables to be governed and managed in a holistic
- manner for the entire enterprise.
- Understand the key concepts in a Process Capability Assessment
- How the COBIT 5 Processes and theProcess Reference Model (PRM) help guide the creation of the 5 Principles and the7 Enablers.

Structure of the Material

- The material is structured in 5 Learning Area Modules
- Based on two specific COBIT 5 Guides
  - ✓ The COBIT 5 ‘Business Framework for the Governance and Managementof Enterprise IT’.
  - ✓ SupplementaryGuide on Process Capability with extracts from the COBIT 4.1 and COBIT 5 PAM’s (ProcessAssessment Model).
  - ✓ Some aspects of the Enabling Process Guide have been used as examplesfor more detailed ‘walk through’where appropriateTips andNotes have been providedin each guide.
- Tips and Notes have been provided in each guide

Exam Requirement and Preparation

- Exam requirements :
  - ✓ 50 Questions
  - ✓ 40 minutes
  - ✓ Closedbook
  - ✓ 50% pass required

- Exam preparation :
  - ✓ Approximately 2 hours
  - ✓ Comprises syllabus review
  - ✓ Test Questions

Questions ?

Overviewof COBIT 5

Major drivers for COBIT 5

Provide more stakeholders a say in determining what they expect from information and related technology

Address the increasing dependency of enterprise success on external business and IT parties such as outsourcers, suppliers, consultants, clients, cloud and other service providers.

Deal with theamount of information, which has increased significantly.

Deal with much more pervasive IT; it is more and more an integral part of the business.

Provide further guidance in the area of innovation and emerging technologies.

Cover the full end-to-end business and IT functional responsibilities.

Get better control over increasing user-initiated and user-controlled IT solutions

Major drivers for COBIT 5

Achieve enterprise:

- Value creation through effective and innovative use of enterprise IT
- Business user satisfaction with IT engagement and services
- Compliancewith relevant laws, regulations, contractual agreements and internal policies
- Improvedrelations between business needs and IT objectives

Connect to, and, where relevant, align with, other major frameworks and standards, such as Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Forum (TOGAF®), Project, Management Body of Knowledge (PMBOK®), Projects IN Controlled Environments 2 (PRINCE2®), Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the International Organization for Standardization (ISO) standards.

Integrate all major ISACA frameworks and guidance, with a primary focus on COBIT, Val IT and Risk IT as one single framework

Benefits

- Information is the business currency of the 21st Century
  - Information has a life cycle: it is created, used, retained, disclosed and destroyed
  - Technology plays a key role in these actions.
  - Technology is becoming pervasive in all aspects of business and personal life.
  - Every form of enterprise needs to be able to rely on quality information to support quality executive decisions!

Enterprise Benefits

Enterprise and their executives strive to:

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

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

Stakeholder Value

- Delivering enterprise stakeholder value requires good **governance and maintenance** of information and technology (IT) assets.
- Enterprise boards, executives and management have to **embrace IT** like any other significant part of the business.
- External **legal, regulatory and contractual compliances** requirements related to enterprise use of information and technology are increasing, threatening value if breached.

- **COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.**

Benefits

- COBIT 5 :
  - ✓Defines the starting point of governance and management activities with the **stakeholder needs** related to enterprise IT.
  - ✓Creates a more holistic, integrated and complete view of enterprise governance and management of IT that is consistent, provides end to end view on all IT-related matters and provides a holistic view.
  - ✓Creates a common language between IT and business for the enterprise governance and management of IT.
  - ✓Is consistent with generally accepted corporate governance standards, and thus helps to meet regulatory requirements.

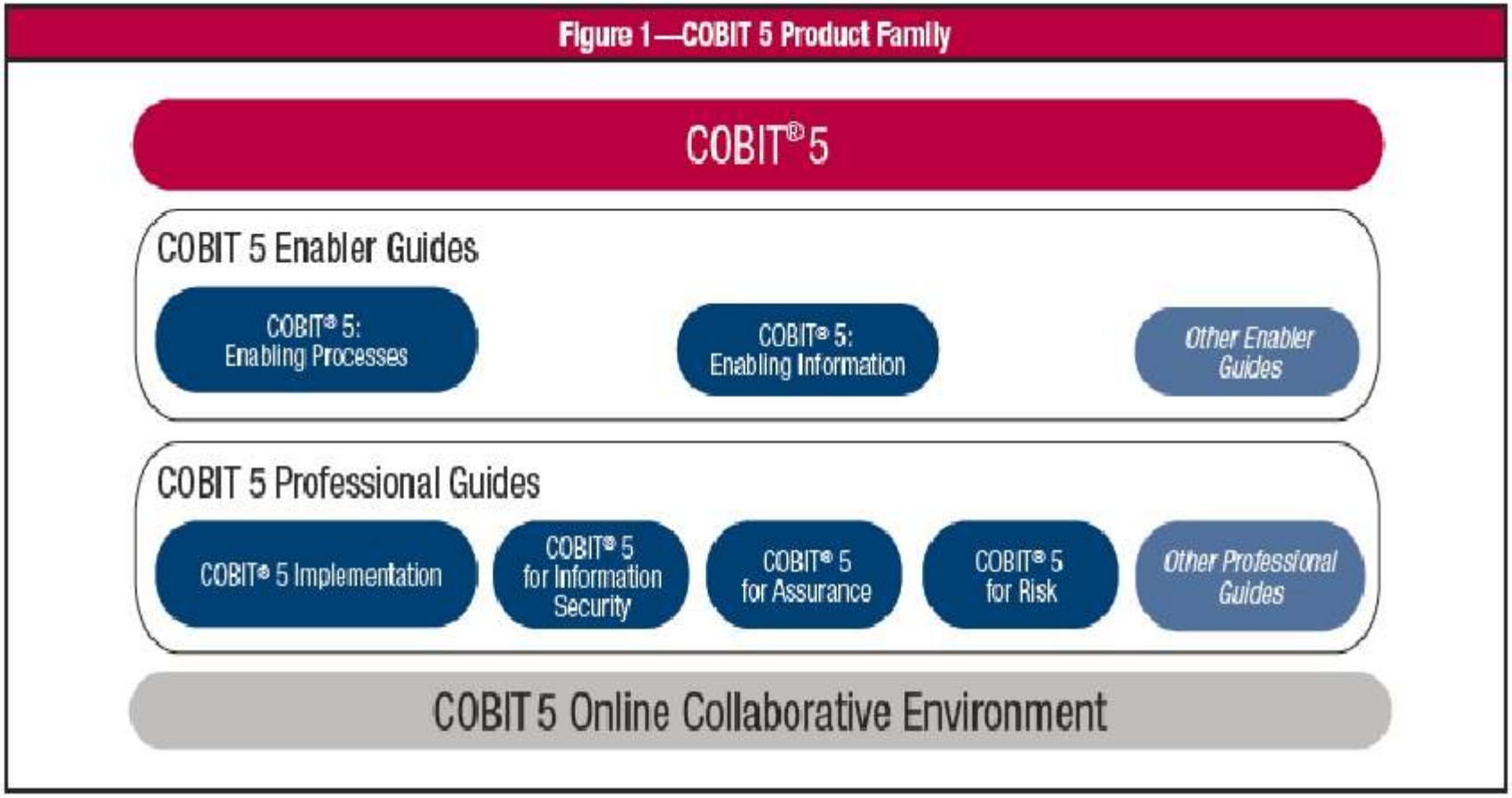
Business Needs

- Enterprises are under constant pressure to:
  - Increase benefits realization through effective and innovation of enterprise IT
    - Generate business value from new enterprise investment with a supportingIT investment.
    - Achieve operational excellence through application of technology.
  - Maintain IT related risk at an acceptable level
  - Contain cost of IT services and technology
  - Ensure business and IT collaboration, leading to business satisfaction with IT engagement and services
  - Comply with ever increasing relevant laws, regulations and policies.

The COBIT 5 Format

- Simplified
  - COBIT 5 directly addresses the needs of the viewer from different perspectives.
  - Development continues with specific practitioner guides
- COBIT 5 is initially in 3 volumes:
  1. The Framework
  2. Process Reference Guide
  3. Implementation Guide
- COBIT 5 is based on:
  - 5 principles and
  - 7 enablers

COBIT 5 Product Family



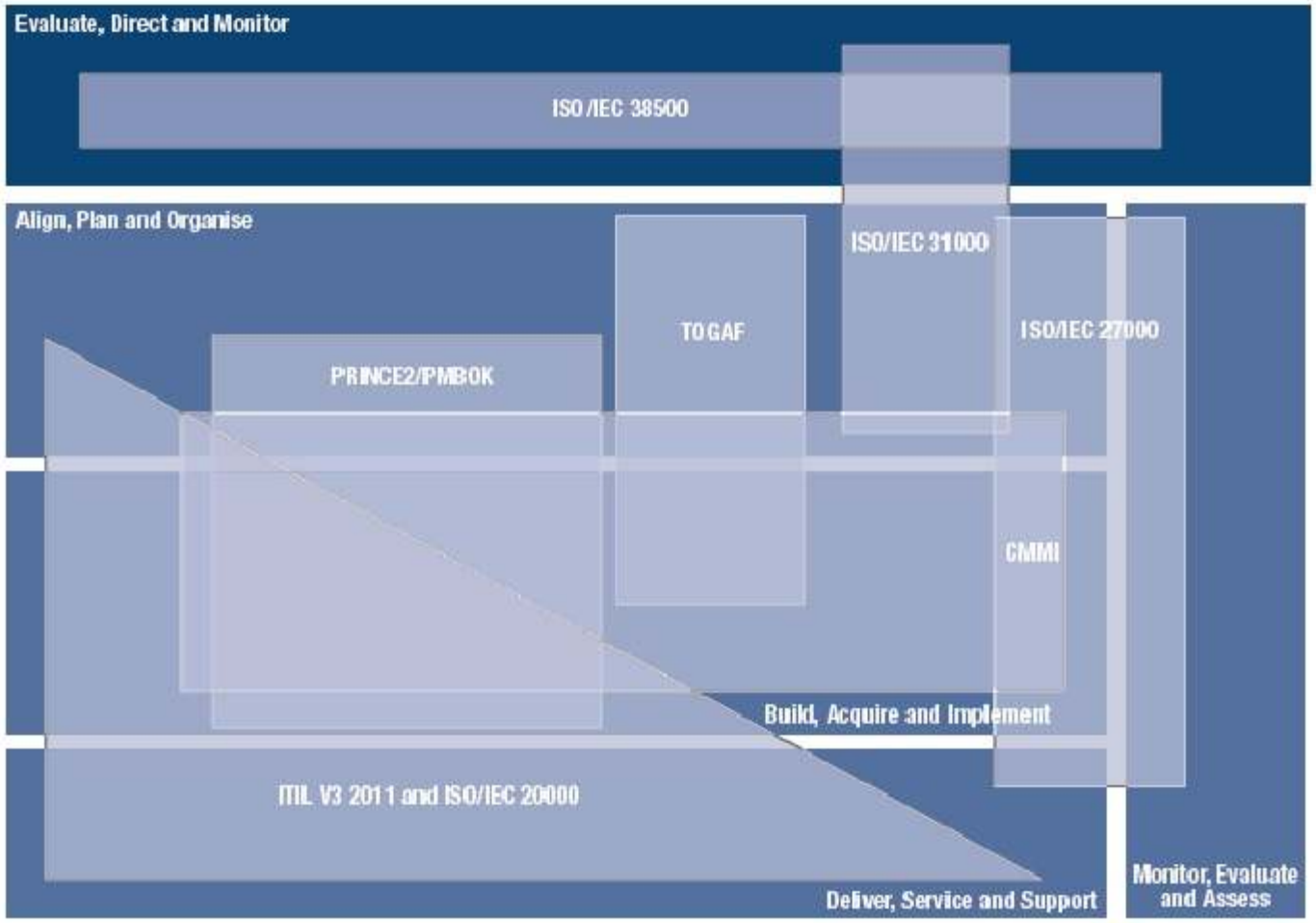
COBIT 5 Product Family

The COBIT 5 product family includes the following products:

- COBIT 5 (the framework)
- COBIT 5 enabler guides, in which governance and management enablers are discussed in detail. These include:
  - COBIT 5: Enabling Processes
  - COBIT 5: Enabling Information (in development)
  - Other enabler guides (check www.isaca.org/cobit)
- COBIT 5 professional guides, which include:
  - COBIT 5 Implementation
  - COBIT 5 for Information Security (in development)
  - COBIT 5 forAssurance (in development)
  - COBIT 5 for Risk (in development)
  - Other professional guides (check www.isaca.org/cobit)
- A collaborative onlineenvironment, which will be available to support the use of COBIT 5

COBIT 5 Mapping Summary

Figure 25—COBIT 5 Coverage of Other Standards and Frameworks



COBIT 5 Mapping Specifies

- ISO/IEC 38500
  - ✓ ISO's 6 principles map to COBIT 5
- ITILv3 the following 5 areas and domains are covered by ITIL v3:
  - ✓ Asubset of processes in the DSS domain
  - ✓ Asubset of processes in the BAI domain
  - ✓ Some processes in theAPO domain
- ISO/IEC 27000
  - ✓ Security and IT- related processes in domainsEDM,APO and DSS
  - ✓ Some monitoringof security activities in MEA
- ISO/IEC 31000
  - ✓ Risk management related activities in EDM andAPO

COBIT 5 Mapping Specifies

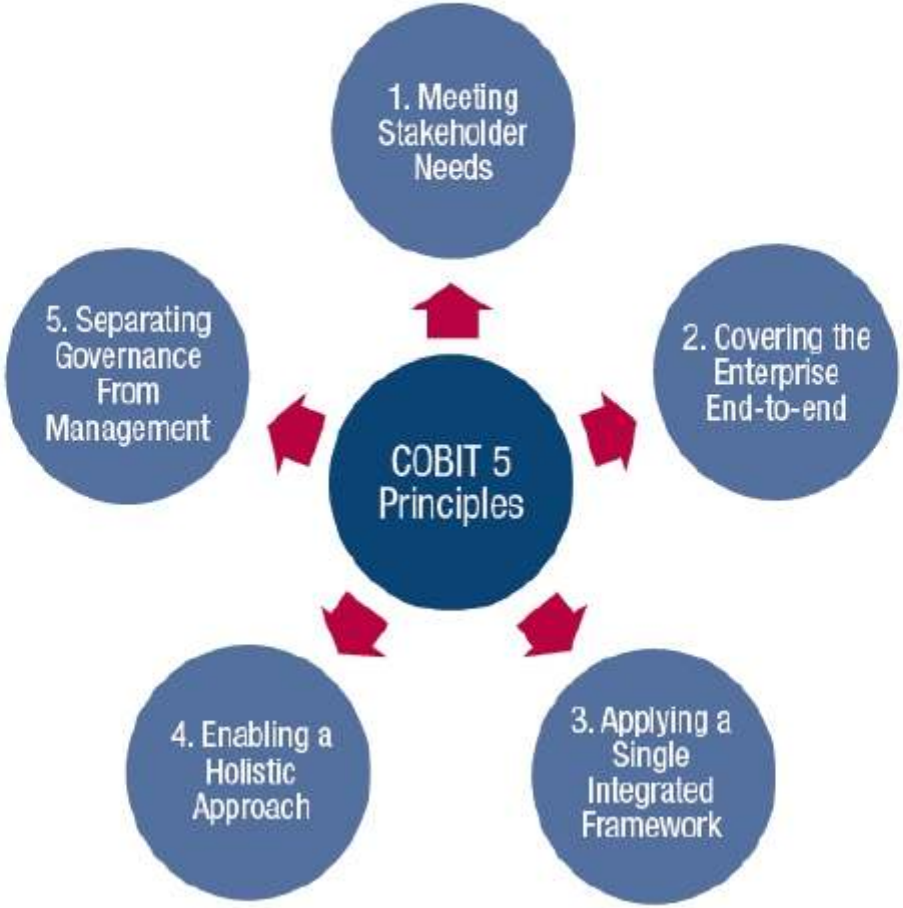
- TOGAF (The Open Group Architecture Framework)
  - ✓ TOGAF componentsof the architecture board and governanceareas.
  - ✓ Resource related processes in EDM
  - ✓ Enterprisearchitecture processes ofAPO
- PRINCE2
  - ✓ Programmeand project managementprocesses in the BAI domain
  - ✓ Portfoliorelated processes in the APO domain
- CMM1
  - ✓ Some organizational and quality related processes in the APO domain
  - ✓ Application building and acquisition related processes in BAI

Questions ?

COBIT 5 PRINCIPLES

COBIT 5 Principles

Figure 2—COBIT 5 Principles

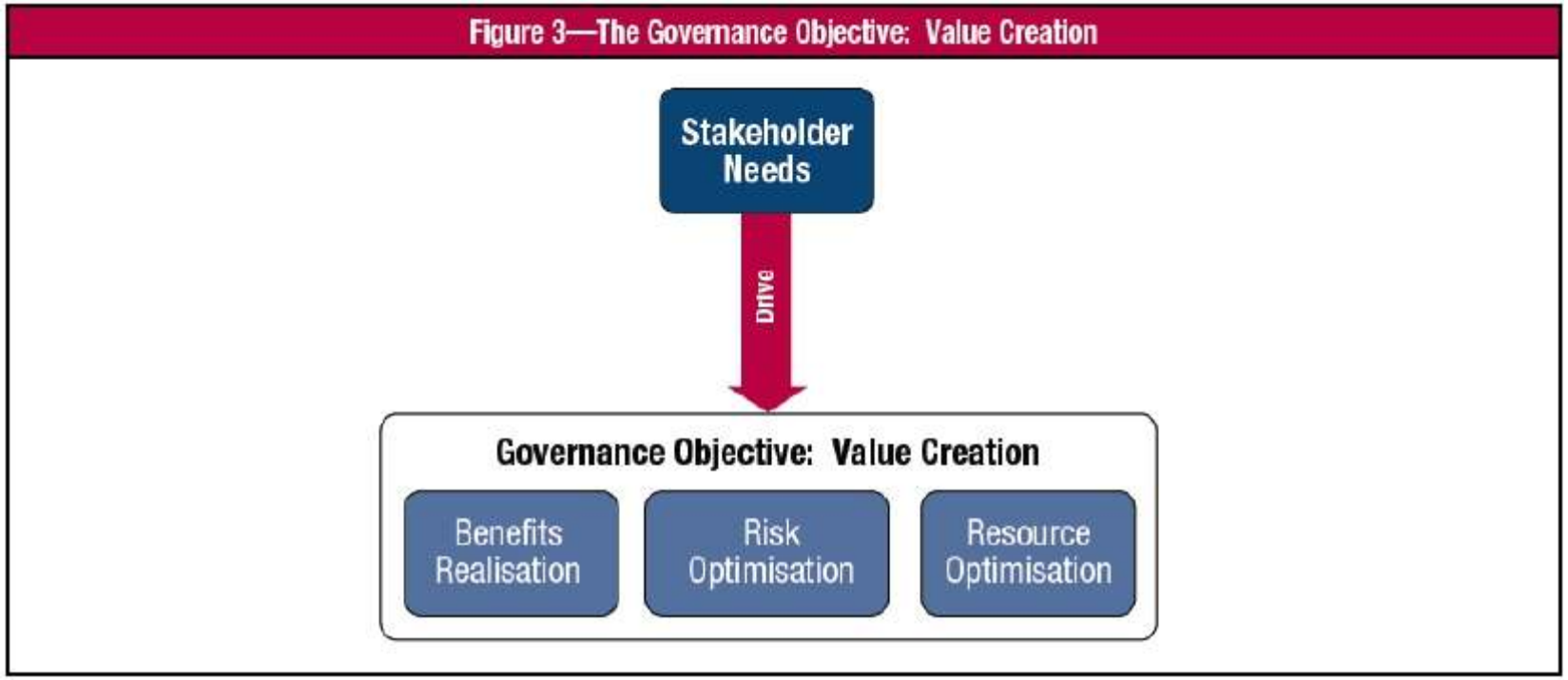


Principle 1: Meeting Stakeholder Needs

- Enterprises have many stakeholders
- Governance is about
  - ✓ Negotiating
  - ✓ Decidingamongst different stakeholder'value interests
  - ✓ Consideringall stakeholderswhen making benefit , resource and risk assessment decisions
- For each decision , ask:
  - ✓ For whom are the benefits?
  - ✓ Who bears the risk?
  - ✓ What resourcesare required?

Principle 1: Meeting Stakeholder Needs

- Enterprises exist to **create value** for their stakeholders



- **ValueCreation** :realizing benefits at an optimal resource cost while optimizing risk.

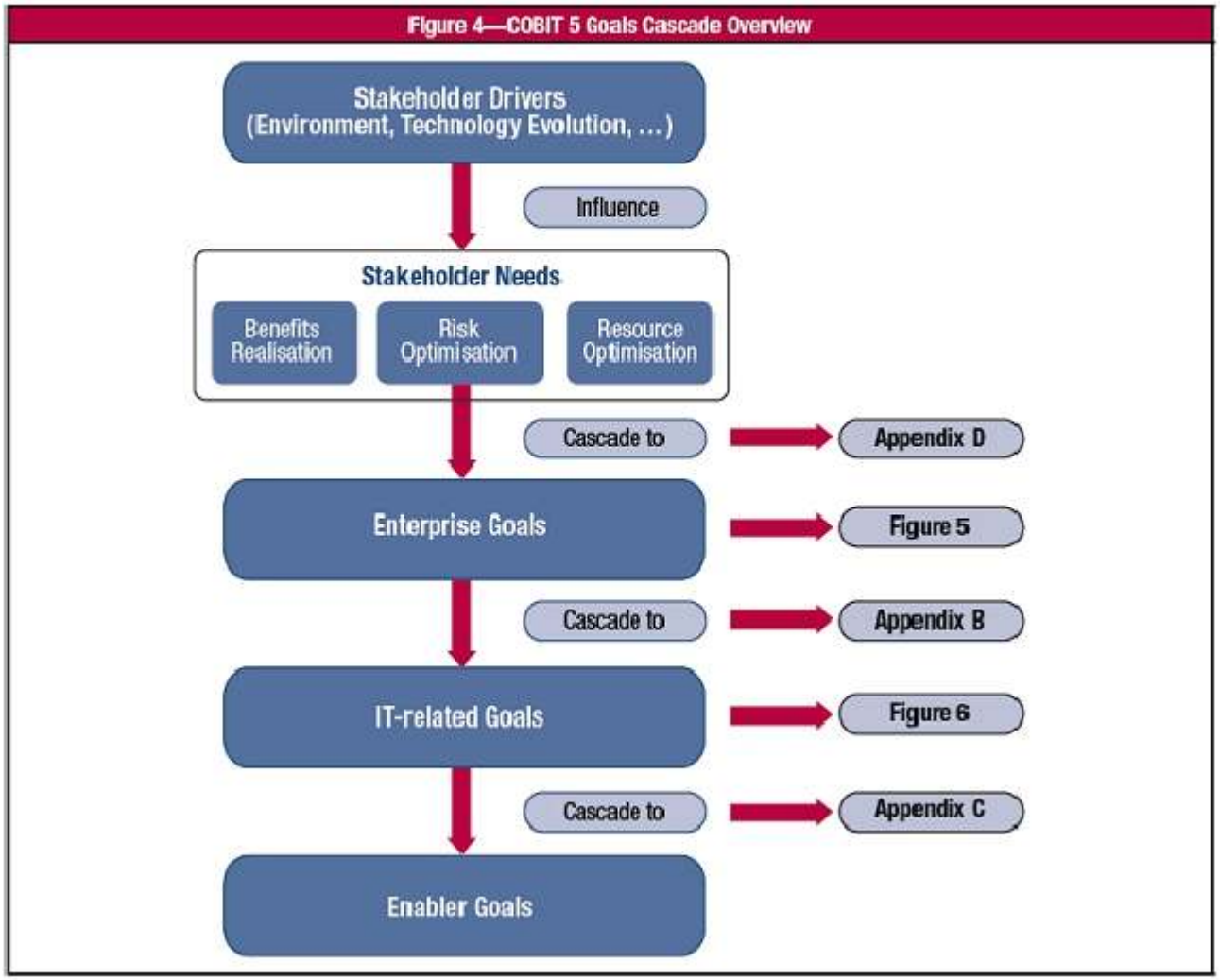
Principle 1: Meeting Stakeholder Needs

- StakeholderNeeds have to be transformed into an enterprises actionable strategy
  - ✓ The COBIT 5 Goals Cascade is the mechanism to translate Stakeholder Needs into specific , practical and customized goals
  - ✓ The COBIT5 goals cascade allows the definition of priorities for
    - Implementation
    - Improvement
    - Assuranceof enterprise governanceof IT

In practice , thegoals 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 assuranceprojects
- ✓ Clearly identifies and communicateshow enablers are used to achieve enterprise goals

COBIT 5 Goals Cascade



COBIT 5 Goals Cascade

Step 1.Stakeholder Drivers Influence Stakeholder Needs

Step 2.Stakeholder Needs Cascade to Enterprise Goals

Step 3.Enterprise Goals Cascade to IT-related Goals

Step 4.IT-related Goals Cascade to Enabler Goals

COBIT 5 Goals Cascade

- **Step 1. Stakeholder Drivers Influence Stakeholder Needs**
  - ✓ Stakeholderneeds are influenced by a numberof drivers, e.g., strategy changes,a changing business and regulatory environment,and new technologies.
- **Step 2. Stakeholder Needs Cascade to EnterpriseGoals**
  - ✓ Stakeholderneeds can be related to a set of generic enterprise goals. These enterprise goals havebeen developedusing the balanced scorecard (BSC) dimensions,and they represent a list of commonlyused goals that an enterprise may define for itself. Although this list is not exhaustive, most enterprise-specific goals can be mappedeasily onto oneor more of the generic enterprise goals.

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

- ✓ The BSC dimension underwhich theenterprise goal fits
- ✓ Enterprise goals
- ✓ The relationship to the three main governance objectives—benefits realization, risk optimization and resource optimization. (‘P’stands for primary relationship and ‘S’for secondary relationship, i.e., a less strong relationship.)

COBIT 5 Goals Cascade

- **Step 3. Enterprise Goals Cascade to IT-related Goals**
  - ✓ Achievement of enterprise goals requires a numberof IT-related outcomes, which are represented by the IT-related goals. IT-related stands for information andrelated technology,and the IT-related goals are structured along the dimensionsof the IT balanced scorecard (IT BSC). **COBIT 5 defines 17 IT-related goals.**

- **Step 4. IT-related Goals Cascade to Enabler Goals**
  - ✓ Achieving IT-related goals requires the successful application and useof a numberof enablers. Enablers include processes, organizational structures and information, and for each enabler a set of specific relevant goals can be defined in supportof the IT-related goals.

COBIT 5 Internal Stakeholders

Figure 7—Governance and Management Questions on IT	
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?

COBIT 5 External Stakeholders

Figure 7—Governance and Management Questions on IT	
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?

Principle 2:
Covering the Enterprise End-to-End

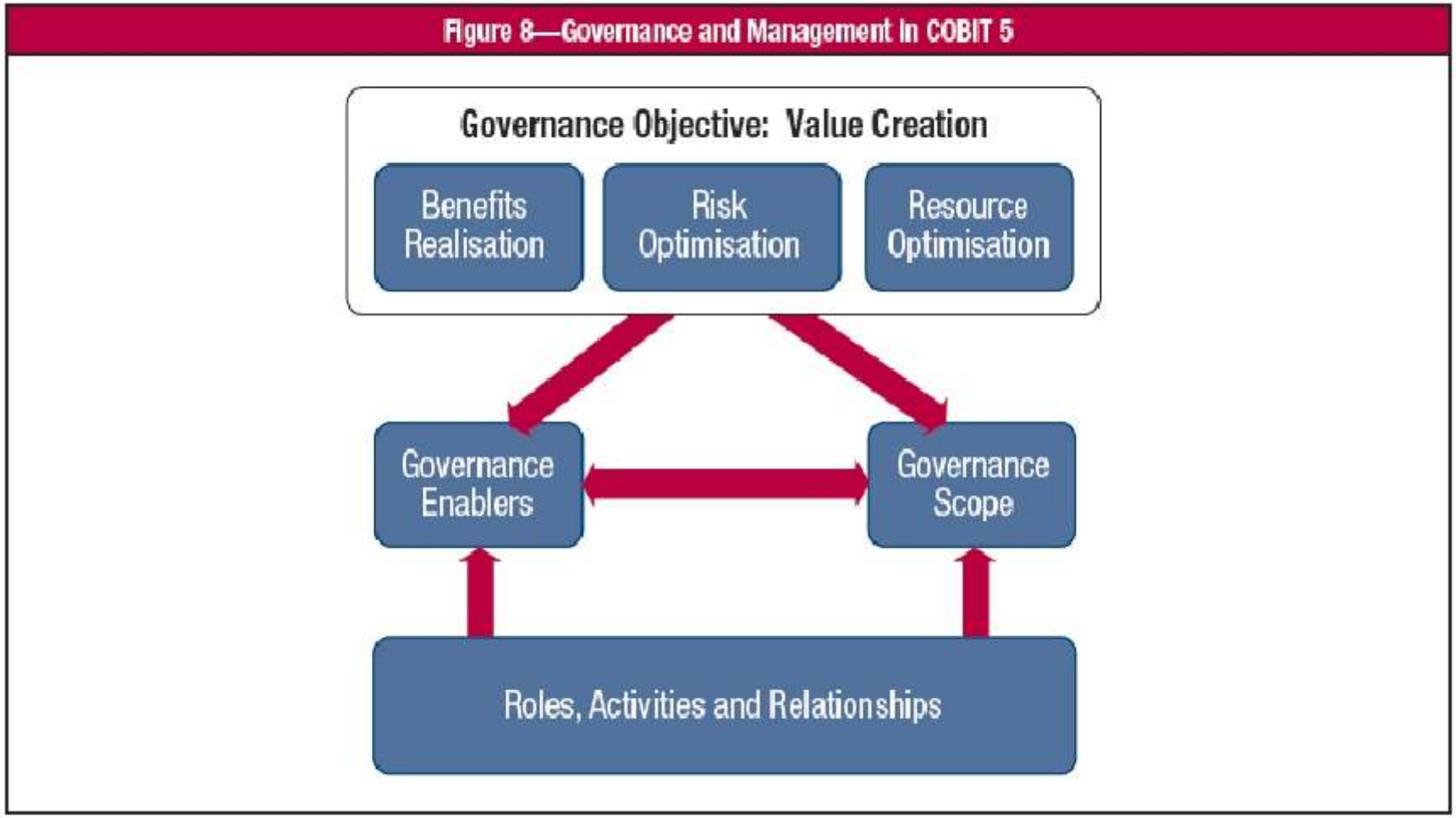
- COBIT 5 addresses the governance and management of information and related technology from an enterprise wide, end-to end perspective

- COBIT 5:
  - Integrates governance of enterprise IT into enterprise governance
  - Covers all functions and processes within the enterprise
  - **Does not focus only on the 'IT Function'**

Principle 2:
Covering the Enterprise End-to-End

- **This means that COBIT 5:**
  - Integrates the governance of enterprise IT into enterprise governance and
  - Covers all functions and processes required to govern and manage enterprise information and related technologies wherever that information is processed.
  - COBIT 5 addresses all relevant interval and external IT services as well as external and internal business processes.

Principle 2:
Covering the Enterprise End-to-End



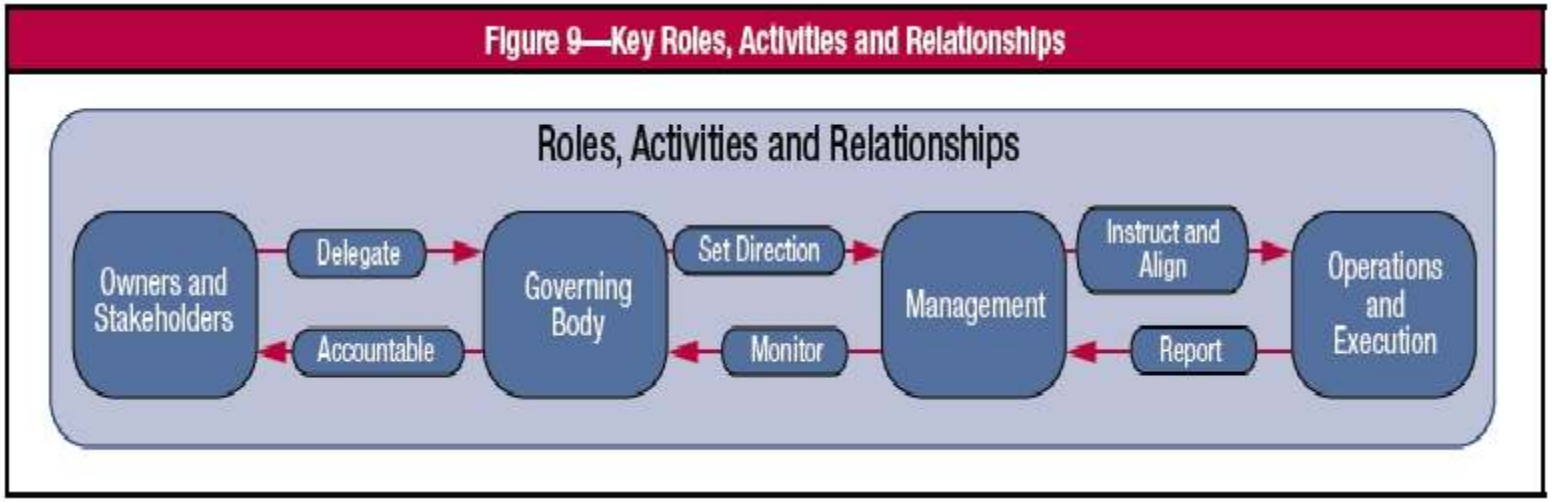
Principle 2:
Covering the Enterprise End-to-End

Main elements of the governance approach:

- Governance Enablers comprising
  - The organizational resources for governance
  - The enterprise's resources
  - A lack of resources or enablers may affect the ability of the enterprise to create value
- Governance Scope comprising
  - The whole enterprise
  - an entity, a tangible or intangible asset ,etc .

Principle 2:
Covering the Enterprise End-to-End

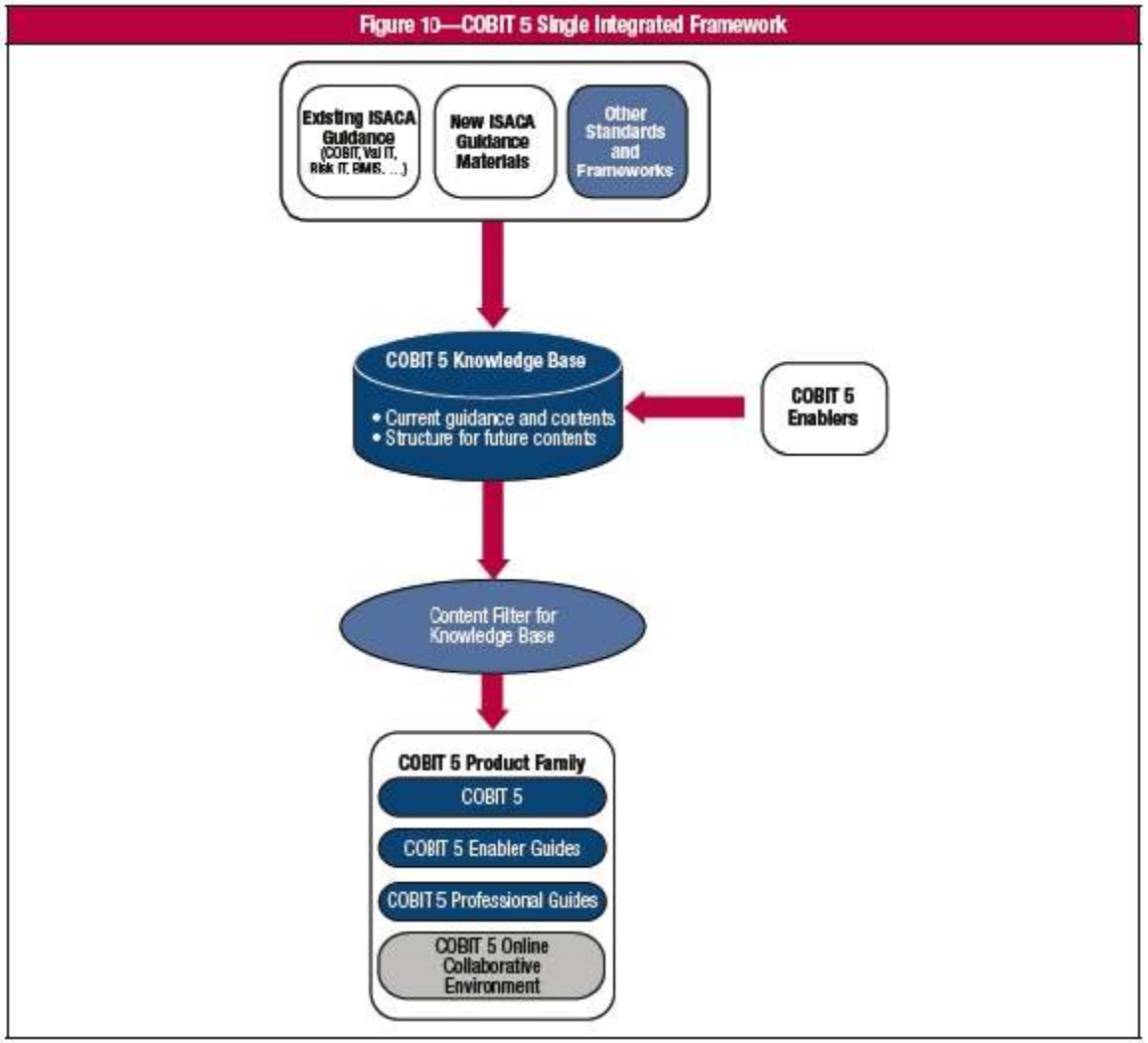
- Governance roles , activities and relationshipsdefine
  - ✓ Whois involved in governance
  - ✓ Howthey are involved
  - ✓ Whatthey do and
  - ✓ Howthey interact
- COBIT 5 defines the difference between governance and management activities in Principle5



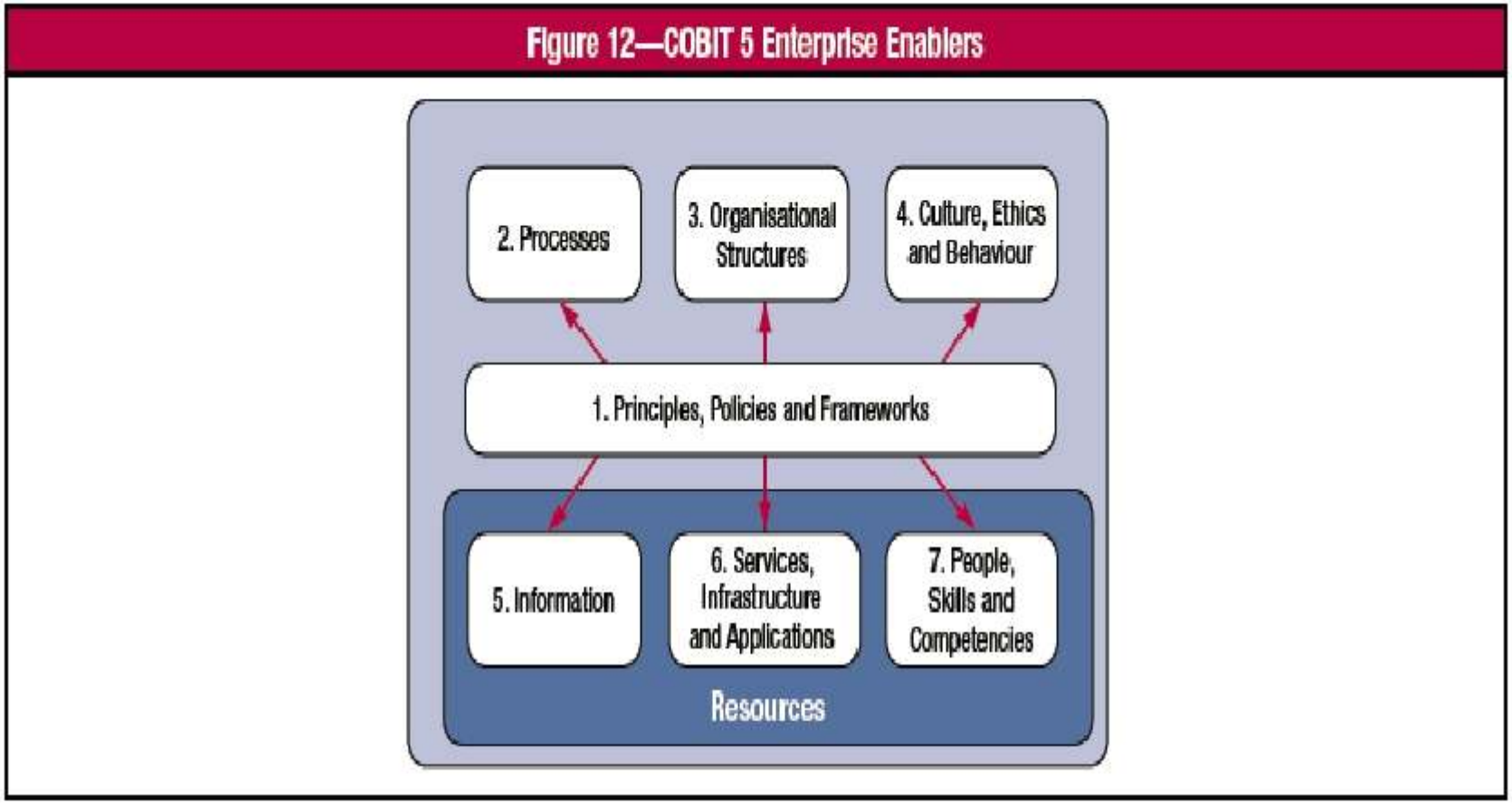
Principle 3:
Applying a Single Integrated Framework

- **COBIT 5:**
  - ✓Aligns with the latest relevant standards and frameworks
  - ✓Is complete in enterprise coverage
  - ✓Provides a basis to integrate effectively other frameworks , standards and practices used
  - ✓Integrated all knowledge previously dispersed over different ISACA frameworks
  - ✓Provides a simple architecture for structuring guidance materials and producing a consistent product set

Principle 3:
Applying a Single Integrated Framework



Principle 4:
Enabling a Holistic Approach



Principle 4:
Enabling a Holistic Approach

Enablers:

1. Principles ,policies and framework
2. Processes
3. Organizational structure
4. Culture,ethics and behavior
5. Information
6. Services ,infrastructure and applications
7. People ,skills and competencies

Principle 4:
Enabling a Holistic Approach

COBIT 5 defines a set of enablers to support the implementation of comprehensive governance and management system for enterprise IT.

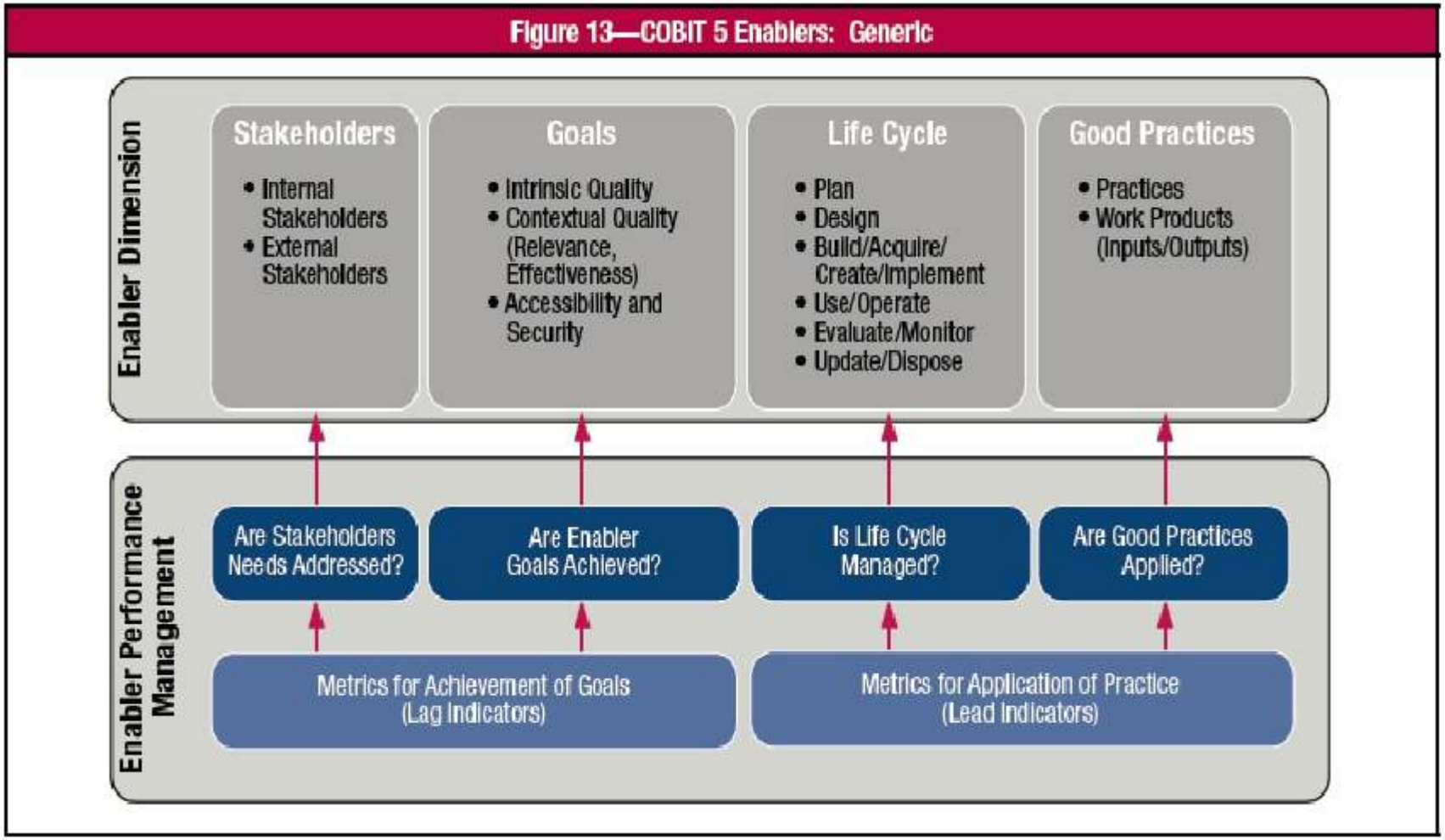
COBIT 5 enablers are:

- Factors that ,individually and collectively, influence whether something will work
- Driven by the **goals cascade**
- Described by the COBIT 5 framework in **seven categories**

COBIT 5 Enabler Dimensions:

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

COBIT 5 Enabler Dimensions:



The Common Dimensions for Enablers:

- **Stakeholders—Each enabler has stakeholders**

  Stakeholders can be internal or external , all having their own, sometimes conflicting, interests
  Stakeholders'needs translate toenterprise goals, which in turntranslate to IT-related goals

Goals—Each enabler has a number of goals, and enablers provide value by the achievement of these goals. Goals can be defined in terms of:

- Expected outcomes of the enabler
  Application or operation of the enabler itself.

The enabler goals are the final step in the COBIT 5 goals cascade.
Goals can be further split up in different categories:

– **Intrinsic quality—**The extent to which enablers work accurately, objectively and provide accurate, objective and reputable results

– **Contextual quality—**The extent to which enablers and their outcomes are fit for purpose given the context in which they operate. For example, outcomes should be relevant, complete, current, 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., access is restricted to those entitled and needing it.

The Common Dimensions for Enablers:

Lifecycle—Each enabler has a life cycle, from inception through an operational/useful life until disposal. This applies to information, structures, processes,policies, etc. The phases of the life cycle consist of:

- Plan (includes concepts developmentand concepts selection)
- Design
- Build/acquire/create/implement
- Use/operate
- Evaluate/monitor
- Update/dispose

Good practices—Foreach of the enablers,good practices can be defined.

- Goodpractices supportthe achievement of the enablergoals. Goodpractices provideexamplesor suggestions on howbest to implement the enabler, and what work productsor inputs and outputsare required. COBIT 5 provides examplesof good practices for someenablers provided by COBIT 5 (e.g., processes).For otherenablers, guidance from otherstandards,frameworks, etc., can be used.

Enabler Performance Management

Enterprises expect positive outcomesfrom theapplication and use of enablers. To manage performance of the enablers,the following questions will have to be monitored and thereby subsequently answered —based on metrics—on a regular basis:

- Are stakeholder needs addressed?
- Are enabler goals achieved?
- Is the enabler life cycle managed?
- Are good practices applied?

The first two bullets deal with the actual outcomeof the enabler. The metrics used to measure to what extent thegoals are achieved can be called **'lag indicators'.**

The last two bullets deal with the actual functioning of the enabler itself, and metrics for this can be called **'lead indicators'.**

Principle 5:
Separating Governance and Management

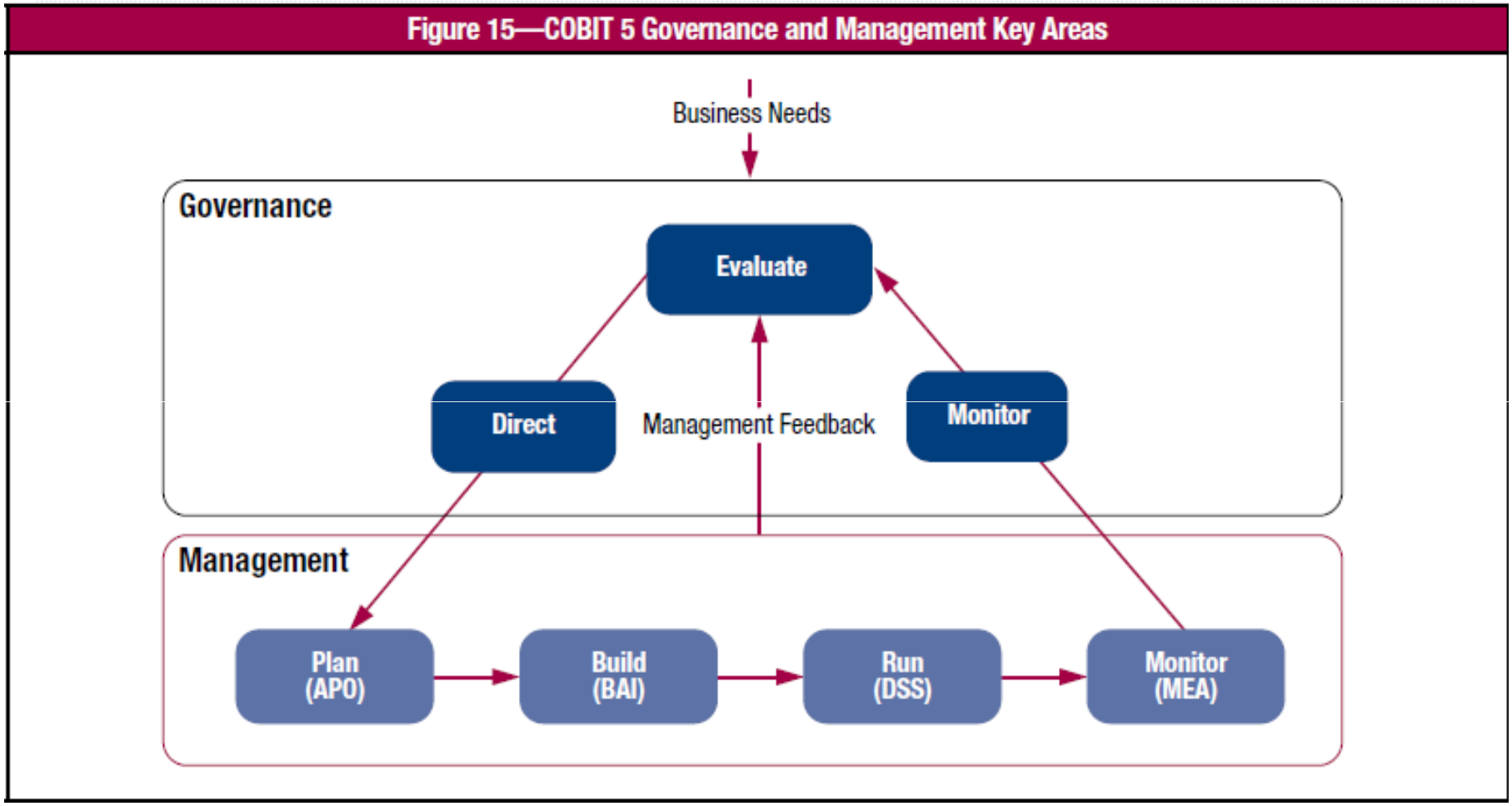
- The **COBIT 5** framework makes a clear distinction between **governance and management**

- **Governance and Management**
  - ✓ Encompass different types of activities
  - ✓ Requiredifferent organizational structures
  - ✓ Servedifferent purposes

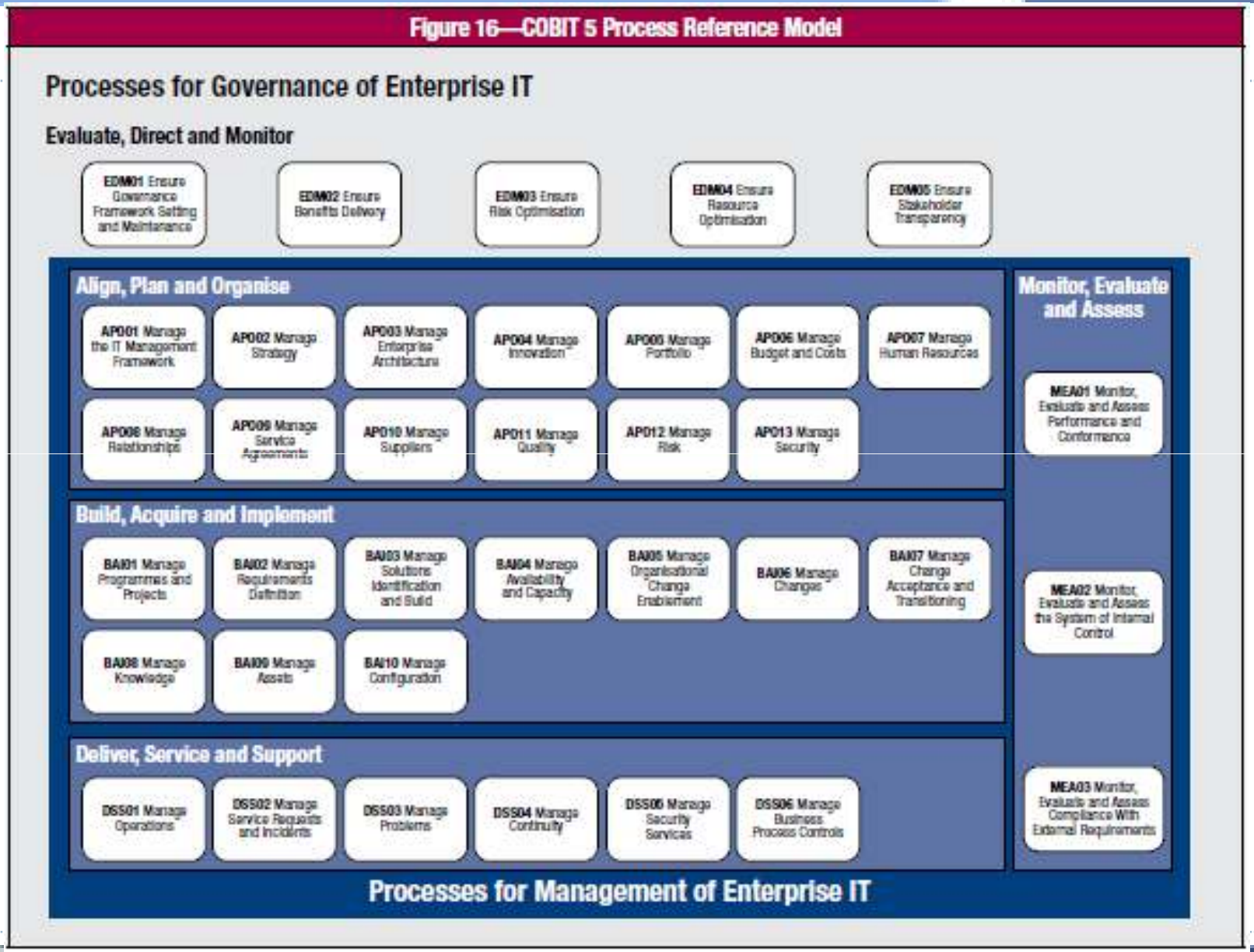
- **COBIT 5 :Enabling Processes** differentiates the activities associated with each domain

Principle 5:
Separating Governance and Management

Figure 15—COBIT 5 Governance and Management Key Areas



COBIT 5: Process Reference Model



Governance & Management

Governance ensures that stakeholder needs, conditionsand options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisationand decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Mostly, governance is the responsibilityof the board of directors under The leadership of the chairperson.

Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the objectives.

Mostly, management is the responsibilityof the executive management underthe leadership of the CEO.

Governance & Management

Governance ensures that stakeholder needs, conditions and options are:

- ✓**Evaluated** to determine balanced ,agreed -on enterprise objectives to be achieved
- ✓Setting **direction** through prioritization and decision making
- ✓**Monitoring** performance ,compliance and progress against agreed direction and objectives **(EDM)**

Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives **(PBRM)**

COBIT 5 IMPLEMENTATION GUIDANCE

COBIT 5 Implementation

ISACA has developed the COBIT 5 Framework to help enterprises implement sound governance enablers.
Implementing good GEIT almost impossible without engaging an effective governance framework.
Best practices and standards are also available to underpin COBIT 5.

However, frameworks, best practices and standards are useful only if they are adopted and adapted effectively.
There are challenges that need to be overcome and issues that need to be addressed if GEIT is to be implemented successfully.

COBIT 5 implementation provides guidance on how to do this .

Enterprise Int & Ext Environment

Understanding the Enterprise Internal and External Environment as they apply to change management such as :

- Ethics and culture
- Applicable laws, regulations, policies
- Mission, vision and values
- Governance policies and practices
- Business plans and strategic intensions
- Operating model
- Management style
- Risk appetite
- Capabilities and available resources
- Industry practices

Key Success factors

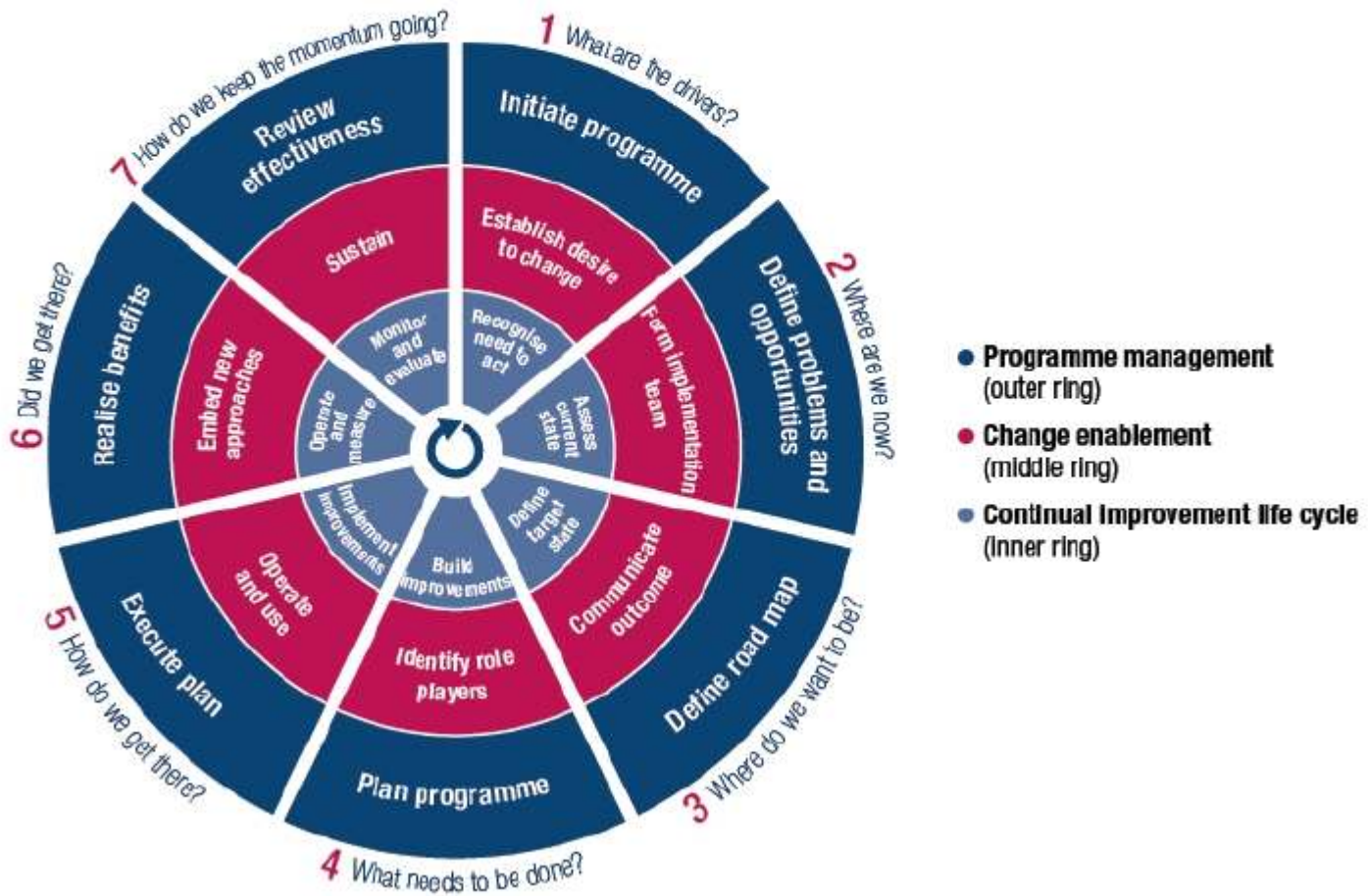
- Top management providing the direction and mandate for the initiative as well as on-going commitment
- All parties supporting the governance and management processes to understand the business and IT objectives
- Ensuring effective communication and enablement of the necessary changes
- Tailoring COBIT and other supporting good practices and standard to fit the unique context of the enterprise and
- Focusing on quick wins and prioritizing most beneficial improvements that are easiest to implement.

Seven Phases – Implementation Life Cycle

- What are the drivers ?
- Where are we now?
- Where do we want to be ?
- What needs to be done ?
- How do we get there?
- Did we get there?
- How do we keep the momentum going ?

COBIT 5 Implementation

Figure 17—The Seven Phases of the Implementation Life Cycle



COBIT 5 Implementation Phases

Phase1 starts with recognizing and agreeing to the need for an implementation or improvement initiative. 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 scopeof the implementation or improvement initiative using COBIT's mapping of enterprise goals to IT-related goals to the associated IT processes, and considering howrisk scenarios could also highlight key processes 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.

During phase 3, an improvement target is set, followed by a more detailed analysis leveraging COBIT's guidance to identify gaps and potential solutions. Some solutions may be quick wins and others morechallenging and longer-term activities. Priority shouldbegiven to initiatives that are easier to achieve and those likely to yield the greatest benefits.

COBIT 5 Implementation Phases

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.

In phase 5, theproposedsolutions are implementedinto day-to-daypractices. Measures can be defined and monitoring established, using COBIT's goals and metrics to ensurethat business alignment is achieved and maintained and performancecan bemeasured. Success requires the engagement and demonstrated commitment of top management as well as ownership by the affected business and IT stakeholders.

Phase 6 focuses on the sustainableoperation of the new or improved enablers and the monitoring of the achievement of expected benefits.

During phase7, the overall success of the initiative is reviewed, further requirements for the governance or management of enterprise IT are identified, and the need for continual improvement is reinforced.

Phase 1:
What are the Drivers ?

- Initiate the programme
- Establish desire to change
- Recognize need to act

Phase 1:
What are the Drivers ?

- Need for new or improved IT governance organization is usually recognized by **pain points or trigger events.**
- Board and executive management should :
  - ✓ Analyze pain points to identify root cause
  - ✓ Look for opportunities during trigger events
- The goal of this phase of the lifecycle includes:
  - ✓ Outlining the business
  - ✓ Identification of stakeholders and roles & responsibilities
  - ✓ ITgovernance program “wake-up call” and kick-off communications.

Typical Pain Points

- ✓ Failed IT initiatives
- ✓ Rising costs
- ✓ Perception of low business value for IT investments
- ✓ Significant incidents related to IT risk (e.g. data loss)
- ✓ Service delivery problems
- ✓ Failure to meet regulatory or contractual requirements
- ✓ Audit findings for poor IT performance or low service levels
- ✓ Hidden and /or rogue IT spending
- ✓ Resources waste through duplication or overlap in IT initiatives
- ✓ Insufficient IT resources
- ✓ IT staff burnout/ dissatisfaction
- ✓ IT enabled changes frequent falling to meet business needs (late deliveries or budget overruns)
- ✓ Multiple and complex IT assurance efforts
- ✓ Board members or senior managers that are reluctant engage with IT.

Relevant Trigger Events

- ✓ Merger,acquisition or divestiture
- ✓ Shift in market,economy or competitiveposition
- ✓ Changein business operating model or sourcing arrangements
- ✓ New regulatory or compliance requirements
- ✓ Significant technology change or paradigm shift
- ✓ An enterprise wise governance focus or project
- ✓ Anew CIO,CFO,COO
- ✓ External audit or consultant assessments
- ✓ Anew business strategy or priority

By using pain points or trigger events as the launching point for IT Governance initiatives; the business case for GEIT improvements can berelated to issues being experienced which will improve buy-into thebusinesscase

Phase 2:
Where are We now ?

- Definethe problems and opportunities **[Programme management]**
  - ✓ Understand the pain points that have been identified as governance problems
  - ✓ Take advantages of trigger events that provide opportunity for improvement
- Form a powerful guiding team **[change enablement]**
  - ✓ Knowledge of business environment
  - ✓ Insight into influencing factors
- Assess the current state **[continual improvement lifecycle attribute]**
  - ✓ Identify theIT goals in respect to enterprise goals
  - ✓ Identify themost important processes
  - ✓ Understand management risk appetite
  - ✓ Understand the maturity of existing governance
  - ✓ Related processes

Phase 3:
Where Do We Want To Be?

- Define the roadmap
  - ✓ Describe thehigh level change enablement plan and objectives
- Communicate desired vision
  - ✓ Develop a communication strategy
  - ✓ Communicate thevision
  - ✓ Articulate the rationaleand benefits of the change
  - ✓ Setthe tone at the top
- Define target state and perform gap analysis
  - ✓ Definethe target for improvement
  - ✓ Analyze the gaps
  - ✓ Identify potentialimprovements

Phase 4:
What Needs To Be Done?

- Develop program plan
  - ✓ Prioritize potential initiatives
  - ✓ Developformal and justifiable projects
  - ✓ Use plans that include contribution and programobjectives
- Empower role players and identify quick wins
  - ✓ High benefit , easy implementationsshould come first
  - ✓ Obtain buy-in by key stakeholders affected by the change
  - ✓ Identifystrengths in existing processes and leverage accordingly.
- Design and build improvements
  - ✓ Plot improvementsonto a grid to assist with prioritization
  - ✓ Consider approach,deliverables , resourcesneeded , costs, estimated time scales, project dependenciesand risks.

Phase 5:
How Do We Get There ?

- Execute the plan
  - ✓ Execute projects according to an integrated program plan
  - ✓ Provide regular update reports to stakeholders
  - ✓ Documents and monitor the contribution of projects while managing risks identified
- Enable operation and use
  - ✓ Build on the momentum and credibility of quick wins
  - ✓ Plan cultural and behavioral aspects of the broader transition
  - ✓ Define measures of success
- Implement improvements
  - ✓ Adopt and adapt best practices to suit the enterprise's approach to policies and process changes

Phase 6:
Did We Get There?

- Realize benefits
  - ✓ Monitorthe overall performanceof the program against business case objectives
  - ✓ Monitorand measure the investment performance
- Embed new approaches
  - ✓ Provide transition from project mode to business as usual mode
  - ✓ Monitor whether new roles and responsibilities have been taken on
  - ✓ Trackand assess objectives of the change response plans
  - ✓ Maintain communicationand ensure communicationbetween appropriatestakeholders continues
- Operated and measure
  - ✓ Set targets for each metric
  - ✓ Measure metrics against targets
  - ✓ Communicateresults and adjust targets as necessary

Phase 7:
How Do We Keep Momentum

- Continual improvements – keeping the momentum is critical to sustainment of the lifecycle
- Review the program benefits
  - ✓ Review programeffectiveness througha programreview gathered
- Sustain
  - ✓ Consciousreinforcement(reward achievers)
  - ✓ Ongoingcommunication campaign (feedback on performance)
  - ✓ Continuoustop management commitment
- Monitor and evaluate
  - ✓ Identifynew governanceobjectives based on programexperience
  - ✓ Communicatelessons learned and further improvementrequirements forthe next iteration of the cycle

Making the Business Case

Importance of a good business case :

The importance of a business case cannot be overstated. An appropriate level of urgency needs to be instilled and the key stakeholders should be aware of the risk of not taking action.An initiative should be owned by a sponsor(senior), involve all key stakeholders, and be based on a business case.

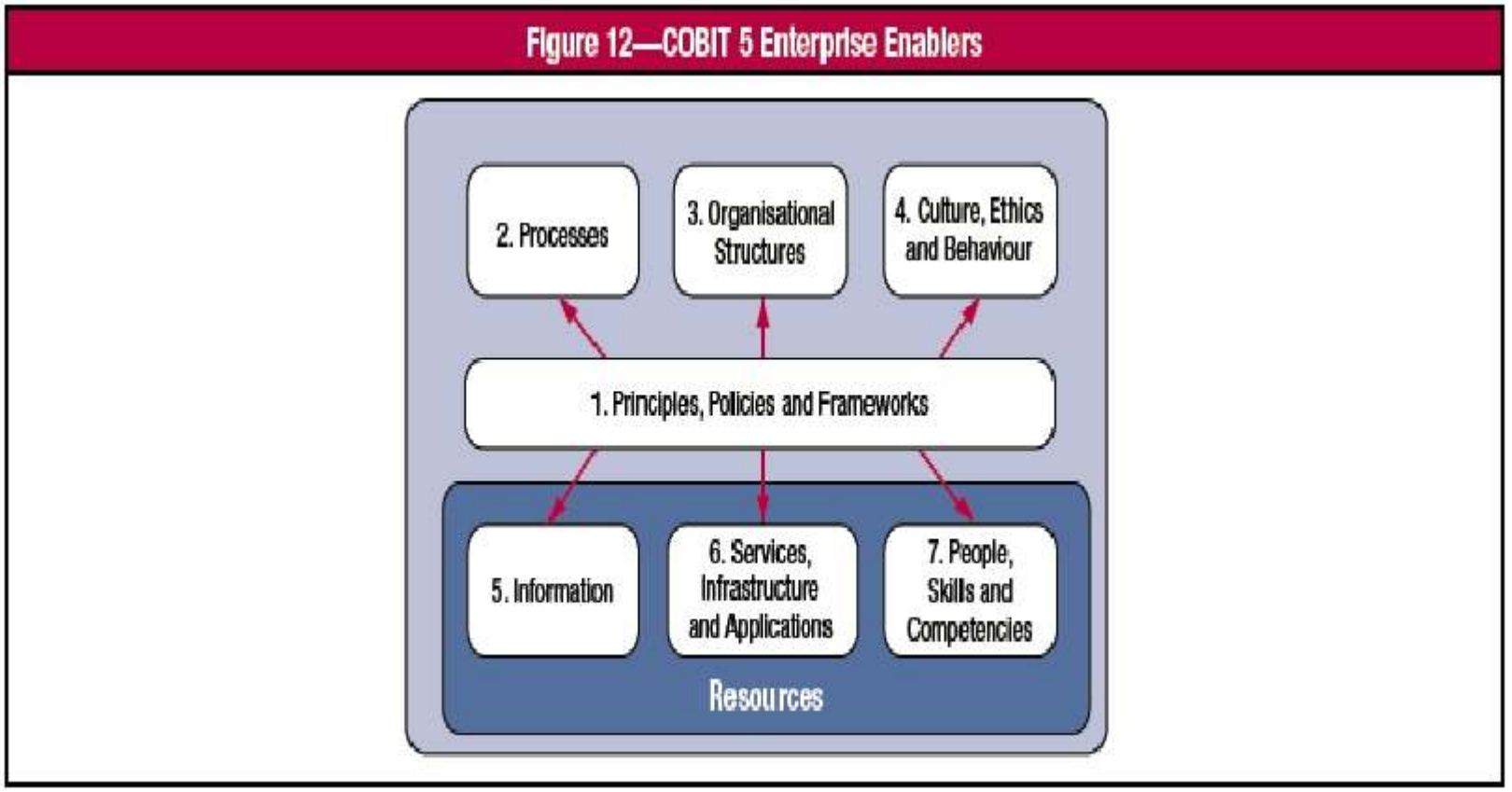
Initially this can be a high- level business case dealing with the strategic benefits and costs and then progress to a more detailed business case. It is a valuable tool available to management in guiding the creation of business value.

Characteristics of Good Business Case

- At a minimum a Business case should include :
  - ✓ The business benefits that will be realized
  - ✓ The business changes required
  - ✓ The investments needed
  - ✓ The on-going IT operating costs
  - ✓ Constraints and dependencies delivered from the risk Assessment
  - ✓ Roles, responsibilities and accountabilities relative to other initiative.
  - ✓ How the investment will be monitored.

COBIT 5 ENABLERS

The COBIT 5 Enterprise Enablers



Recap Principle 4 : Enabling a Holistic Approach:

Enablers

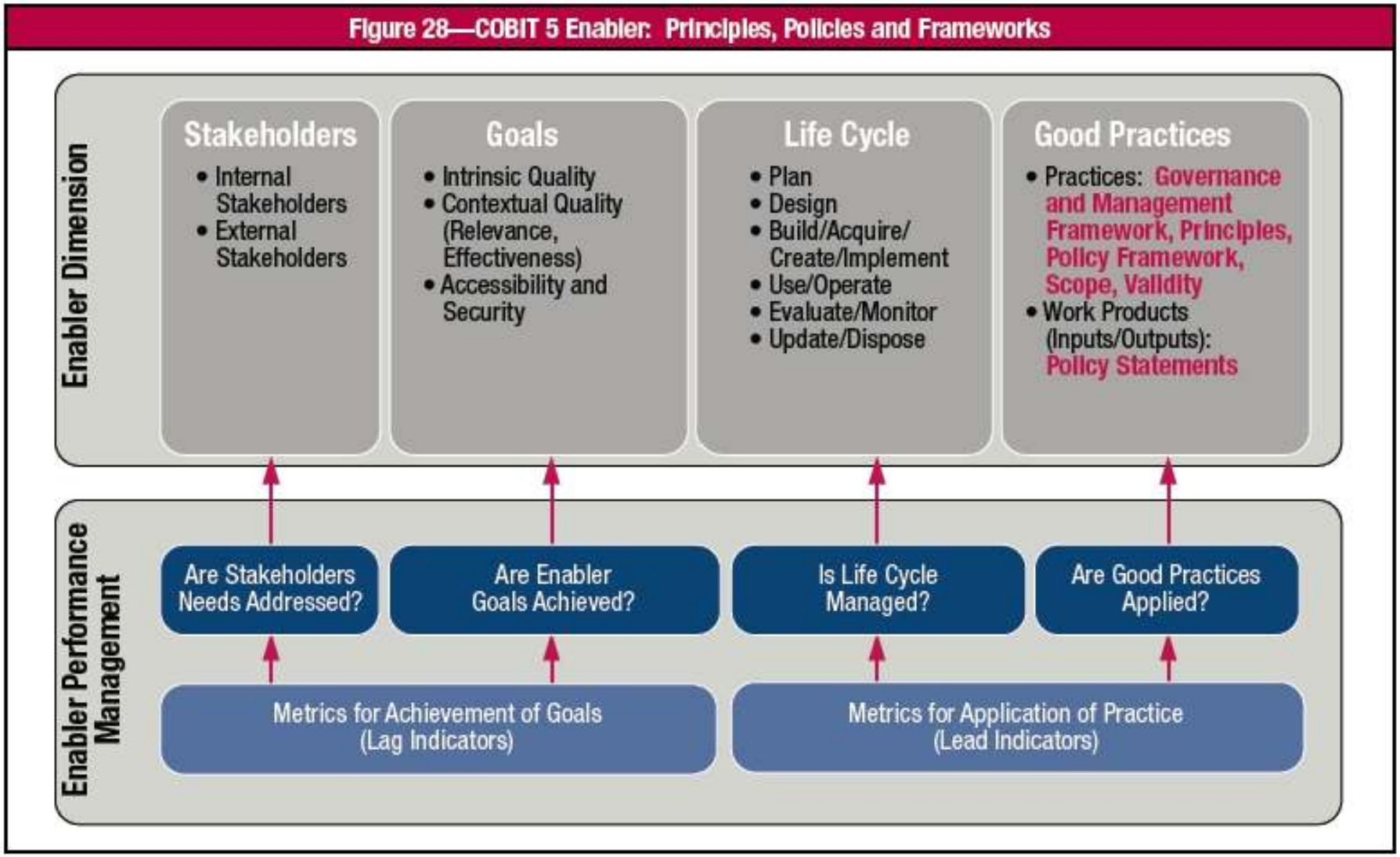
1. Principles, policies and frameworks
2. Processes
3. Organizational structures
4. Culture, ethics and behavior
5. Information
6. Services, infrastructure and applications
7. People, skills and competencies

Recap Principle 4 : Enabling a Holistic Approach:

COBIT5 enabler dimensions :

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

Enabler 1:
Principles, Policies & Framework



Enabler 1:
Principles, Policies & Framework

- The purpose of this enabler is to convey the governing body's management direction and instructions . They are instruments communicate the rules of the enterprise , in support of the governance objectives and enterprise values as defines by the board and executive management.

- Differences between principles and policies –
  - Principlesneed to be limited in number
  - Putin simple language , expressing as clearly as possiblethe core values of the enterprise
  - Policiesare more detailed guidance on how to put principles into practice

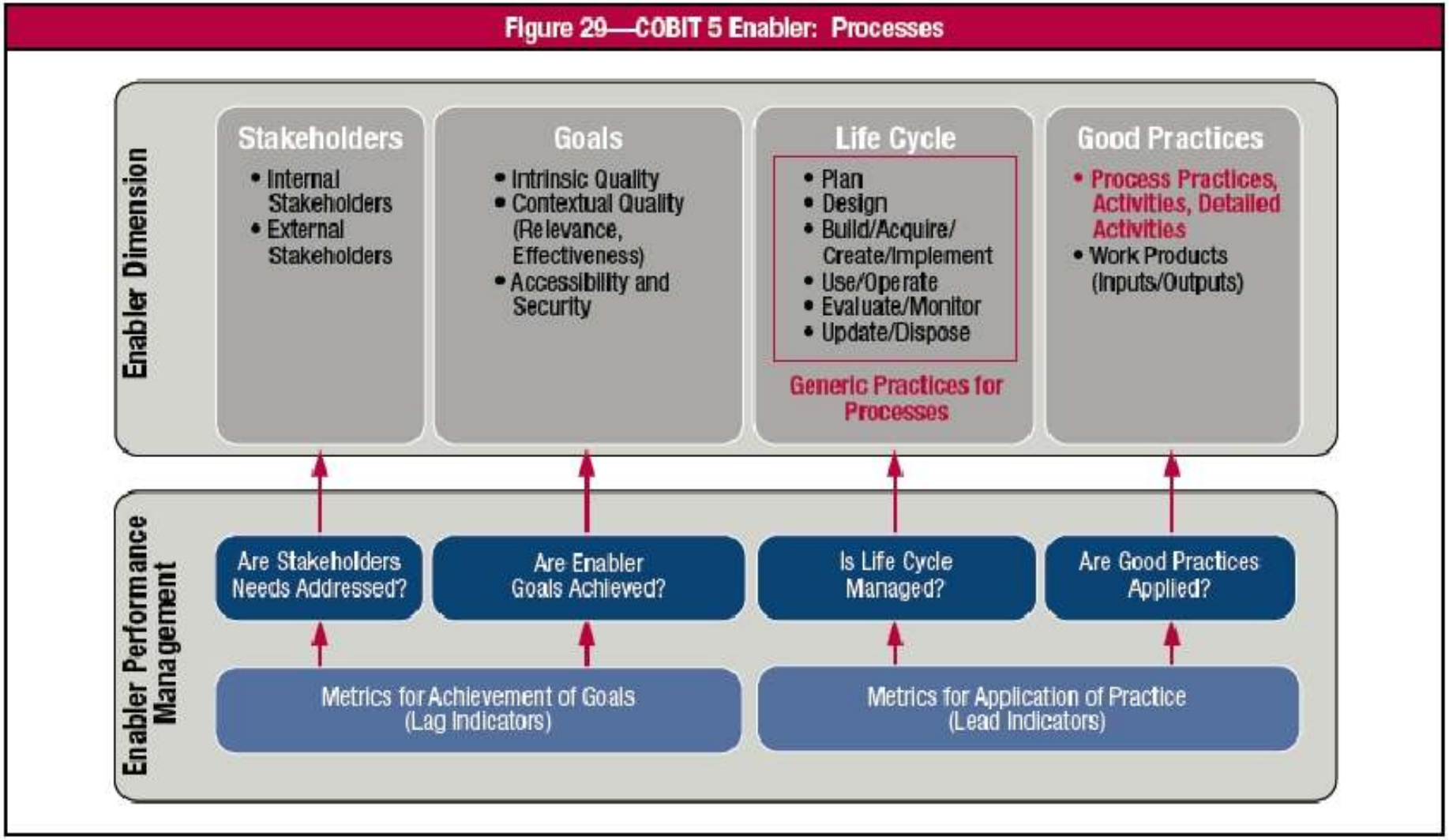
Enabler 1:
Principles, Policies & Framework

- The characteristics of good policies ; they should
  - ✓ Be effective – achieve their purpose
  - ✓ Be efficient – especially when implementing them
  - ✓ Non-intrusive – Should make sense and be logical to those who have to comply with them
- Policies should have a mechanism (framework) in place where they can be effectively managed and users know where to go. Specifically they should be :
  - ✓ Comprehensive, covering all required areas
  - ✓ Open and flexible allowing for easy adaptation and change.
  - ✓ Current and up to date
- The purpose of a policy life cycle is that it must support a policy framework in order to achieve defined goals.

Enabler 1:
Principles, Policies & Framework

- The Good Practice Requirements for policies and frameworks, are important, specifically :
  - ✓ Their Scope
  - ✓ Consequences of falling to comply with the policy
  - ✓ The means of handling exceptions
  - ✓ How they will be monitored
- The links and relationships between principles, policies and frameworks and other enablers :
  - ✓ Principles, policiesand frameworks reflect the culture,ethics and valuesof the enterprise
  - ✓ Processesare the most important vehiclefor executingpolicies
  - ✓ Organizationalstructures can defineand implement policies
  - ✓ Policiesarepart of information

Enabler 2: Processes



Enabler 2 Process - Definitions

- **A process is defined** as a collection of practices influences by the enterprises policies, and procedures that takes inputs from a number of sources(including other processes) manipulates the inputs and produces outputs(e.g. products and services)
- **Process Practices** are defined s the ‘guidance’ necessary to achieve process goals.
- **ProcessActivities** are defined as the ‘Guidance’ to achieve management practices for successful governance and management of enterprise IT.

- **Inputs and Outputs** are the process work products/ artifacts considered necessary to support operation of the process.

Enabler 2: Processes

- Each process is divided into :
  - Process description
  - Process Purpose statement
  - IT- related Goals(from the Goals cascade see example in the Appendix)
  - Each IT- related goal is associated with a set of generic related metrics
  - Process goals (Also from the goals cascade mechanism and is referred to as Enabler goals)
  - Each process contains a set of Management Practices
  - These are associated with a generic RACI chart (Responsible, Accountable, Consulted, Informed)
  - Each management practices contains a set of inputsand outputs (called work products)
  - Each management Practice is associated with a set of activities

Enabler 2: Processes

- Processes complements COBIT 5 and contains a detailed reference guide to the processes that are defined in the COBIT 5 process reference model:
  - ✓The COBIT 5 goals cascade is recapitulated and complemented with a set of example metrics for the enterprise goals and the IT related goals.
  - ✓The COBIT 5 process model is explained and its components defined.
  - ✓The Enabler process guide which is referenced in this module contains the detailed process information for all 37 COBIT 5 processes shown in the process reference model.

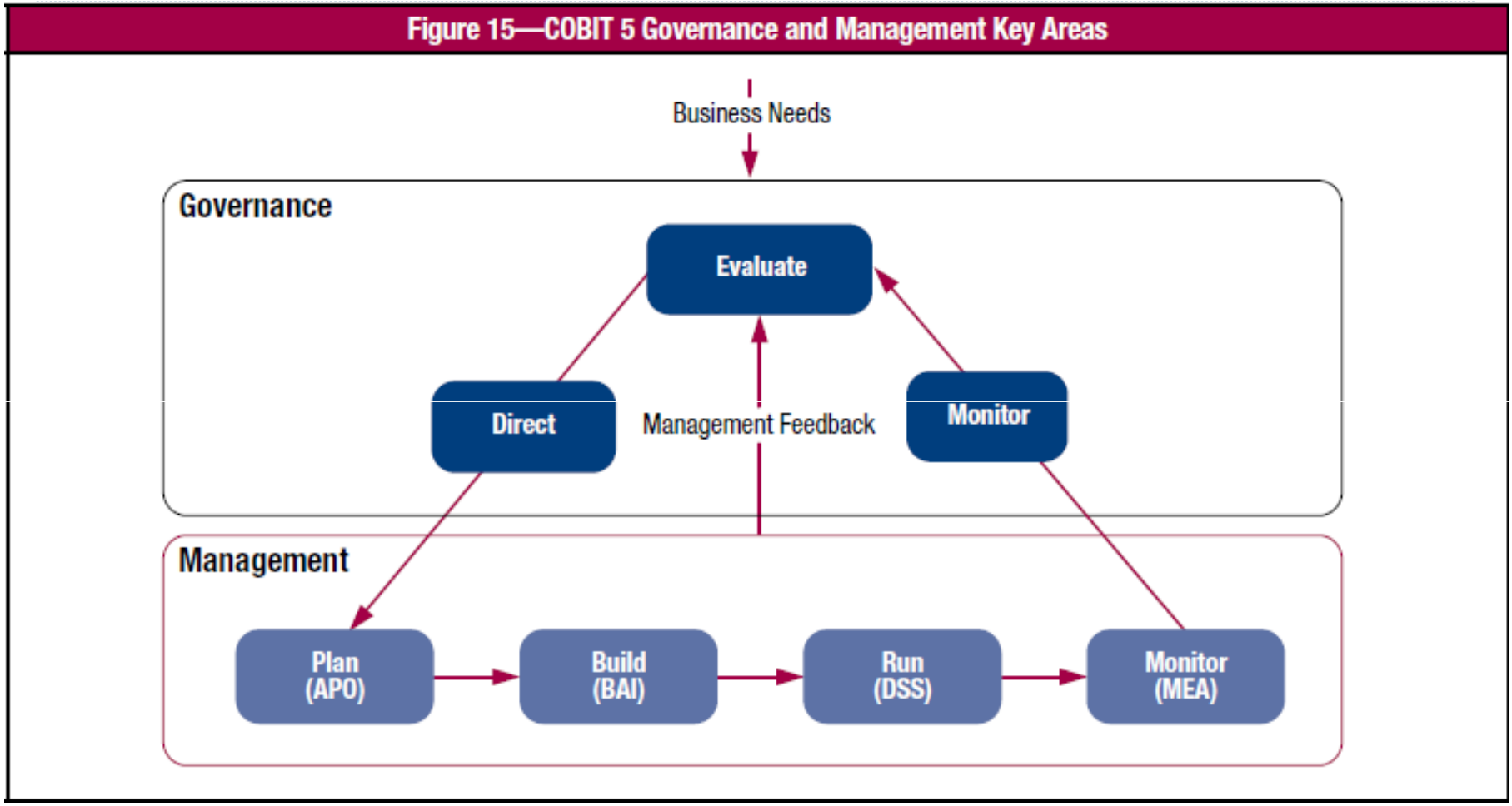
Enabler 2: Processes

COBIT5 : Enabling Processes

- The COBIT 5 process reference model subdivides the IT--related practices and activities of the enterprise into two main areas- governance and management – with management further divided into domains of processes :
  - ✓The GOVERNANCE domain contains five Governance Processes; within each process, evaluate, direct and monitor (EDM) practices are defined.
  - ✓The four MANAGEMENT domains are in line with the responsibility areas of plan, build, run and monitor (PBRM)

COBIT 5 Process Reference Model

Figure 15—COBIT 5 Governance and Management Key Areas



Structure of the PRM Template

(Based on the ISO 15504 process definitions and structure)

- The PRM is divided into a Governance Domain with 5 Processes titled EDM (Evaluate , Direct and Monitor)
- Four management domains titled APO (Align, Plan and Organize); BAI (Build, Acquire and Implement) DSS (Deliver, Service and Support) and MEA (Monitor, Evaluate andAssess)
- APO contains 13 processes, BAI 10 processes, DSS 6 processes and MEA 3 processes
- This makes a total of 37 processes, 32 for management and 5 for Governance

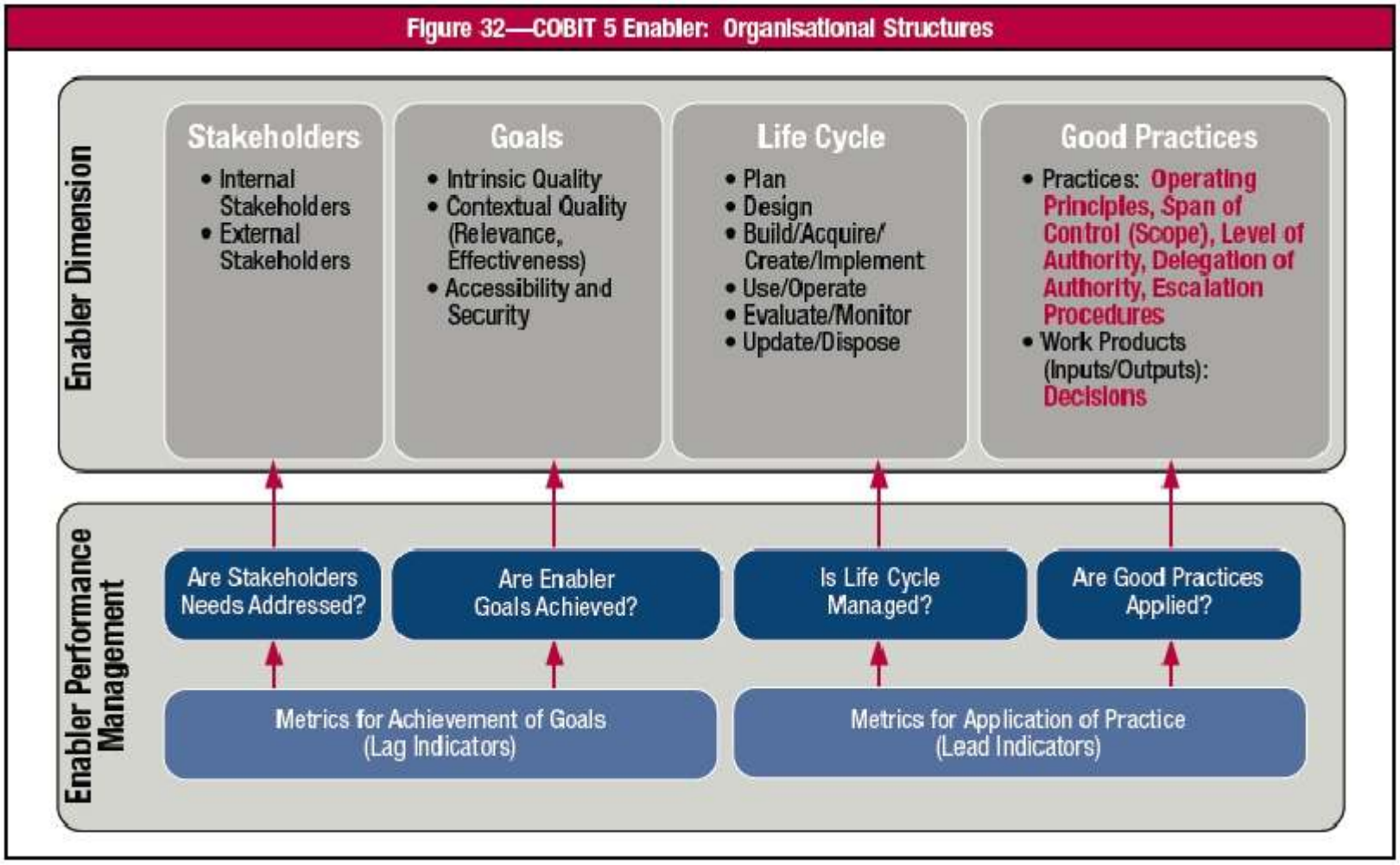
Key Characteristics of Process Goals:

- ProcessGoals are defined as a statement describing the desired outcomeof a process.An outcome can be an artifact, a significant changeof a state or a significant capability improvement of other processes.They are part of the goals cascade in which processgoals link to IT- related goals which link to enterprise goals.
  - Intrinsic Goals
    - ✓ Doesthe process have intrinsic quality? Is it accurate and in line with good practice? Is it compliant with internal and external rules?
  - Contextual Goals
    - ✓ Is the process customized and adapted to the enterprise's specific situation? Is the process relevant, understandable, easy to apply?
  - Accessibility and Security Goals
    - ✓ The process remains confidential, when required, and is known and accessible to those who need it.

Enabler 2: Processes

- Relationship between Process and other enablers:
  - Processes need information as one form of input.
  - Processes need organizational structure.
  - Processes produce and require services, infrastructure and applications
  - Processes are dependent on other processes.
  - Processes need policies and procedures to ensure consistent implementation.

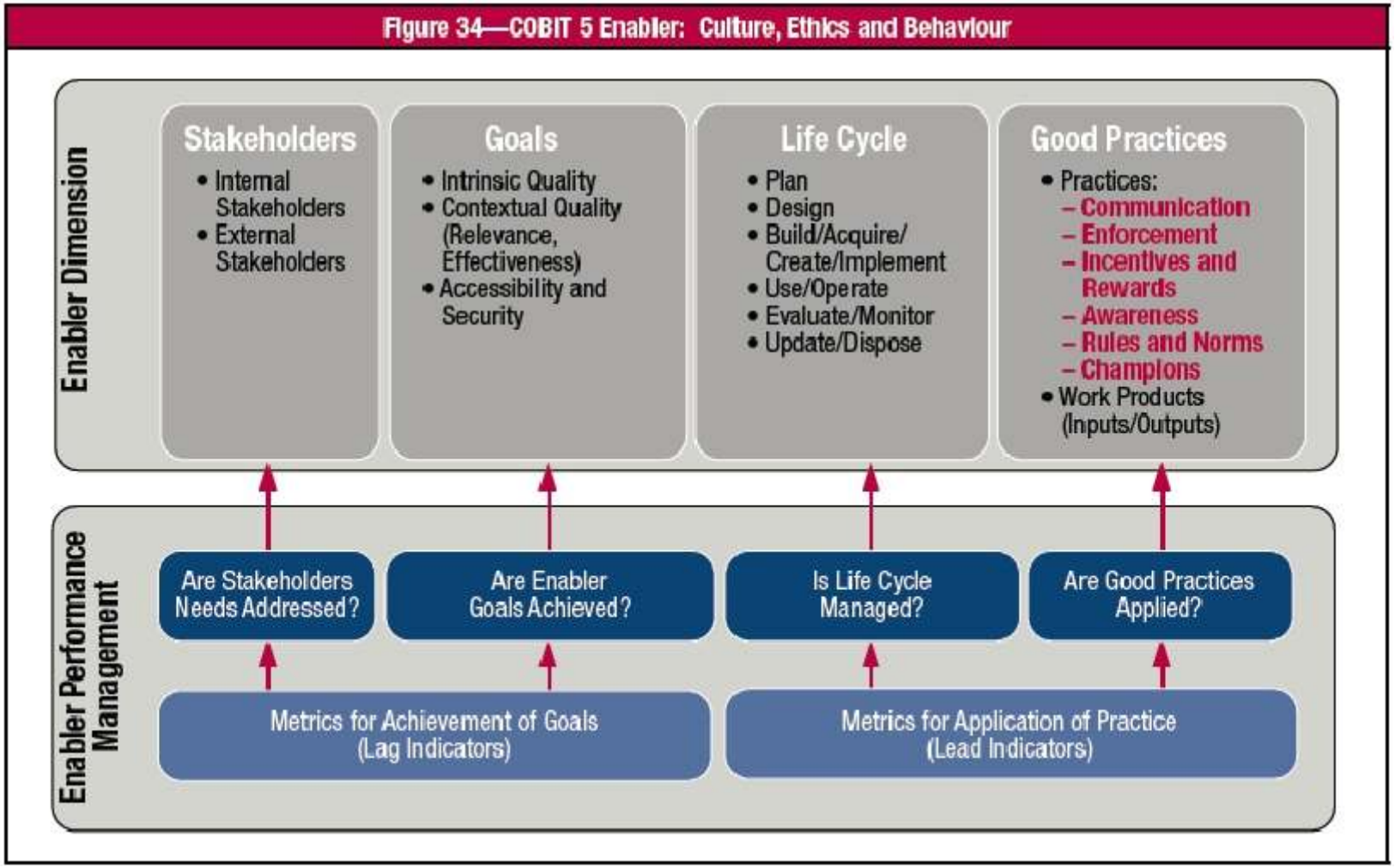
Enabler 3: Organizational Structures



Enabler 3: Organizational Structures

- A number of Good Practices of organizational structure can be distinguished such as :
  - ✓ Operating principles – The practical arrangements regarding how the structurewill operate, such as meeting frequency documenting and other rules.
  - ✓ Span of control- The boundaries of theorganization structure's decisionrights.
  - ✓ Level of authority – the decisions that the structure is authorized to take.
  - ✓ Delegation of responsibility– The structure can delegate a subset of its decisionrights to other structures reporting to it.
  - ✓ Escalatingprocedures – The escalating path for a structure describes therequired actions in case of problems in making decisions.

Enabler 4: Culture, Ethics and Behavior



Enabler 4: Culture, Ethics and Behavior

- Good practices for creating, encouraging and maintaining desired behavior throughout the enterprise include:
  - ✓ Communication throughout the enterprise of desired behaviors corporate values.(This can be donevia a code of ethics).
  - ✓ Awareness of desired behavior, strengthened by senior manager . Example. This is one of thekeys to a good governance environment when senior management and theexecutives walk the talk so to speak. It is sometimes a difficult areas and one that causes many enterprises tofail because it leads to poorgovernance. (Typically will be part of a trainingand awareness sessions around areas of ethics)
  - ✓ Incentives to encourage and deterrents to enforce desired behavior. There is a clear link to HR payment and reward schemes.
  - ✓ Rulesand norms which provide more guidance and will typically be found in a Code of Ethics.

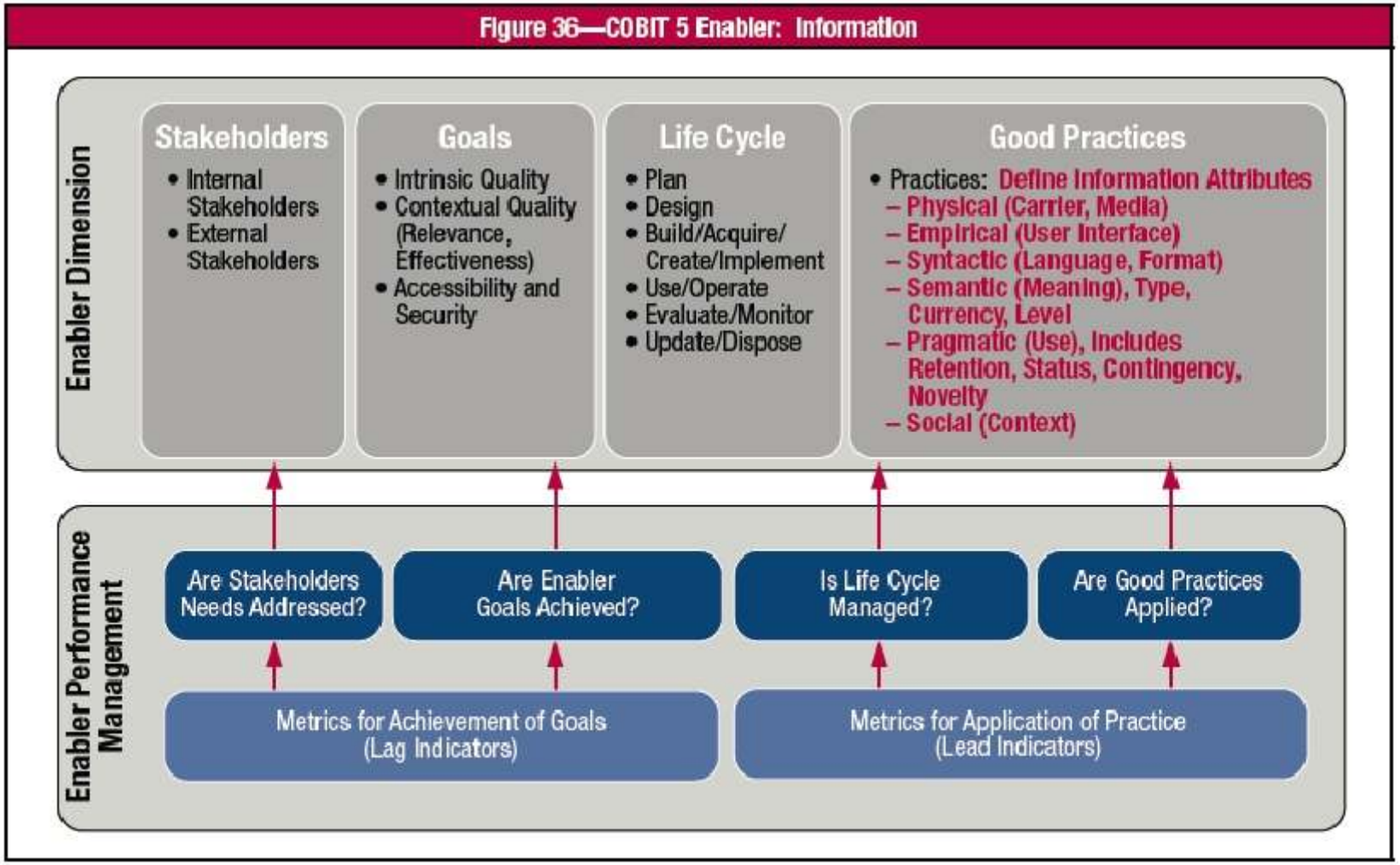
Enabler 4: Culture, Ethics and Behavior

- Relationship of Goals for culture, ethics and behavior
  - Organizational Ethics determine by the values by which the enterprise tolive(its code)
  - Individual ethics determined by each person's personal values and dependent to some extent on external factors not always under the enterprise's control such as religion, ethnicity..etc
  - Individual behaviors which collectively determine the culture of the enterpriseand is dependent on both organizational and individual ethics.Some examples are :
    - Behavior towards risk taking
    - Behavior towards the enterprise's principles and policies.
    - Behavior towards negative outcomes, e.g. loss events

Enabler 4:
Culture, Ethics and Behavior

- The relationship of this enabler is to other enablers
  - ✓ Links to processes for execution process activities
  - ✓ Links to organizational structures for the implementation of decisions and
  - ✓ Links to principles and policies to be able to communicate the corporate values.(many organizations include their code of ethics with their policies)

Enabler 5: Information



Enabler 5: Information

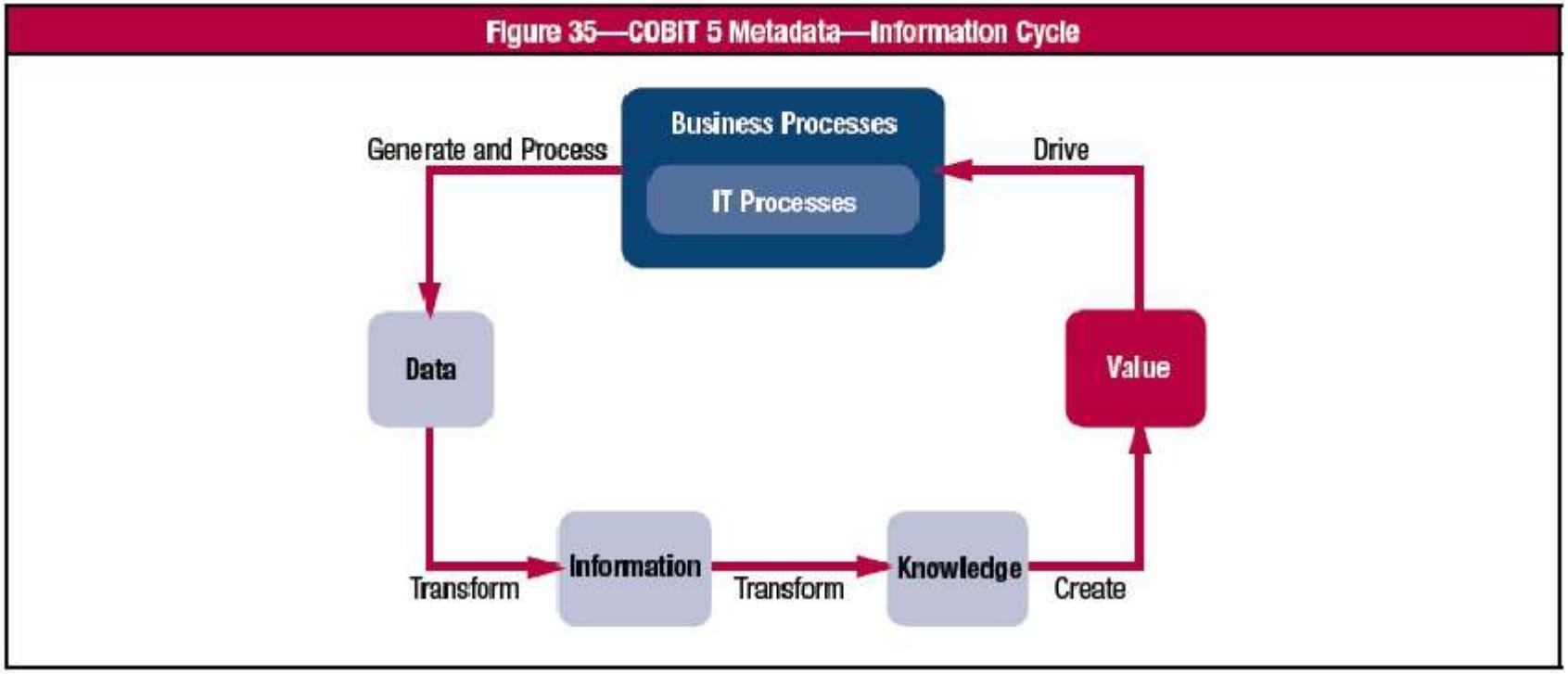
- Information Stakeholders
  - Information producer - responsible for creating the information
  - Information custodian - responsible for storing and maintaining the information
  - Information consumer - responsible for using the information

- **Importance of the Information Quality categories and dimensions;**
  - ✓The concept of information criteria was introduces in COBIT 4.1;these were very important to be able show how to meet business requirements.
- **Importance of Information Criteria**
  - ✓COBIT 4.1 introduces us to the concept of 7 Key information criteria to meet Business requirements. This concept has been retained but translated differently

Enabler 5
The COBIT 4.1 Info Criteria Cube

- To satisfy business objectives, information needs to conform to certain control criteria which COBIT refers to as business requirements for information. Base broader quality, fiduciary and security requirements, seven distinct information criteria are defined. These are:
  - Effectiveness
  - Efficiency
  - Confidentiality
  - Integrity
  - Availability
  - Compliance
  - Reliability

COBIT 5 Enabler 5 Information – Meta data Information Cycle



Information Layers

Information attributes applied to the following layers :

- Physical World Layer – The world where all phenomena that can be empirically observed takes place.
  - **Theattribute that identifiesthe physicalcarrier of the information, e.g., paper, electric signals,soundwaves**

- Empirical layer – The empirical observation of the signs used to information and their distinction from each other.
  - **Theattribute that identifiesthe access channel of the information, e.g., userinterfaces**

Information Layers

- Syntactical Layer – The rules and principles for constructing sentence in natural or artificial language. Syntax refers to the form of information.
  - ✓ **Attribute that identifies the representational language/format usedfor encoding the information and the rules for combining the symbols of the languageto form syntactic structures.**
- Semantic layer – The rules and principles for constructing meaning out of thesyntax structures.
  - ✓ **Semantics refers to the meaning of information.**
    - **Information type—The attribute that identifies the kind of information, e.g., financial vs. non-financial information, internal vs. external origin of the information, forecasted/predicted vs. observed values, planned vs. realized values**
    - **Information currency—The attribute that identifies the time horizon referred to by the information, i.e., information on the past, the present or the future**
    - **Information level—The attribute that identifies the degree of detail of the information, e.g., sales per year, quarter, month**

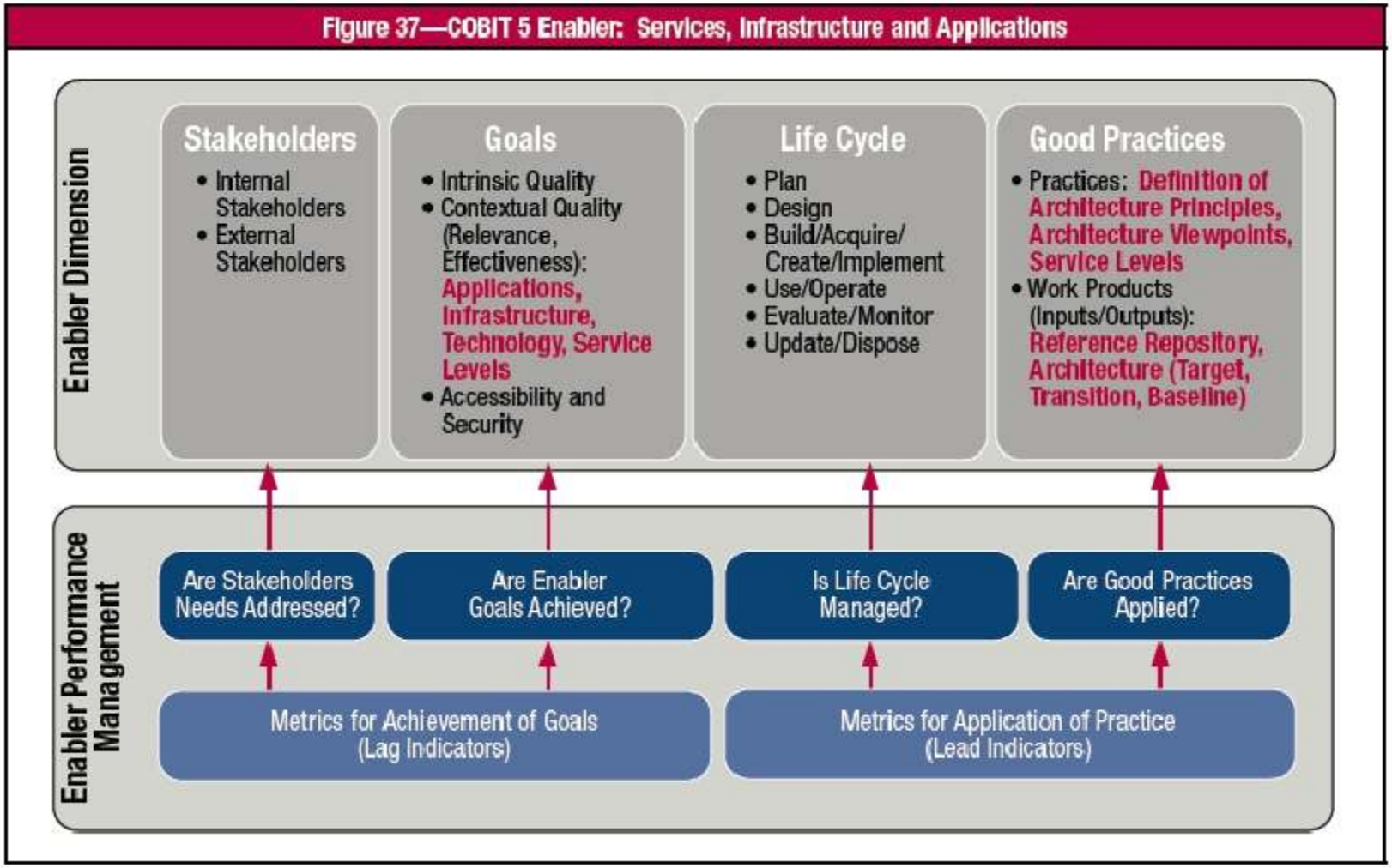
Information Layers

- Pragmatic layer – The rules and structures for constructinglayer languagestructures that fulfill specific purposesin human communication.Pragmatics refersto the use of information.
  - ✓ **Retentionperiod—The attribute that identifies how long information can be retained beforeit is destroyed**
  - ✓ **Information status—The attribute that identifies whether the information is operational orhistorical**
  - ✓ **Novelty—The attribute that identifies whether the information createsnew knowledge orconfirms existing knowledge, i.e., information vs. confirmation**
  - ✓ **Contingency—The attribute that identifies the information that is required to precede this information (for it to be considered as information)**

- Social World layer – The world that is socially constructed the use of languagestructures at the pragmatic level of semi e.g. contracts, laws, culture.
  - The possible used of the Information Model
    - ✓ **Usefor Information Specifications**
    - ✓ **Use to determine required protection**
    - ✓ **Usedto determine easeof data Use.**

Enabler 6: Services, Infrastructure & Applications

Figure 37—COBIT 5 Enabler: Services, Infrastructure and Applications



Architecture Principles

- Five architecture principles govern the implementation and use of IT- Related resources

- This is part of the Good Practices of this enabler

Architecture Principles are :

- **Reuse-** Common components ofthe architecture shouldbe used when designing and implementing solutions as part of the target or transition architectures.
- **Buy vs. build** – Solutions shouldbe purchasedunless there is an approved rationale for developing them internally.
- **Simplicity** – The enterprise architecture shouldbe designed and maintained to besimple as possiblewhile still meeting enterprise requirements.
- **Agility-** The enterprise architecture shouldincorporate agility to meet changing business needs in an effective and efficient manner.
- **Openness**– The enterprise architecture shouldleverage open industry standards.

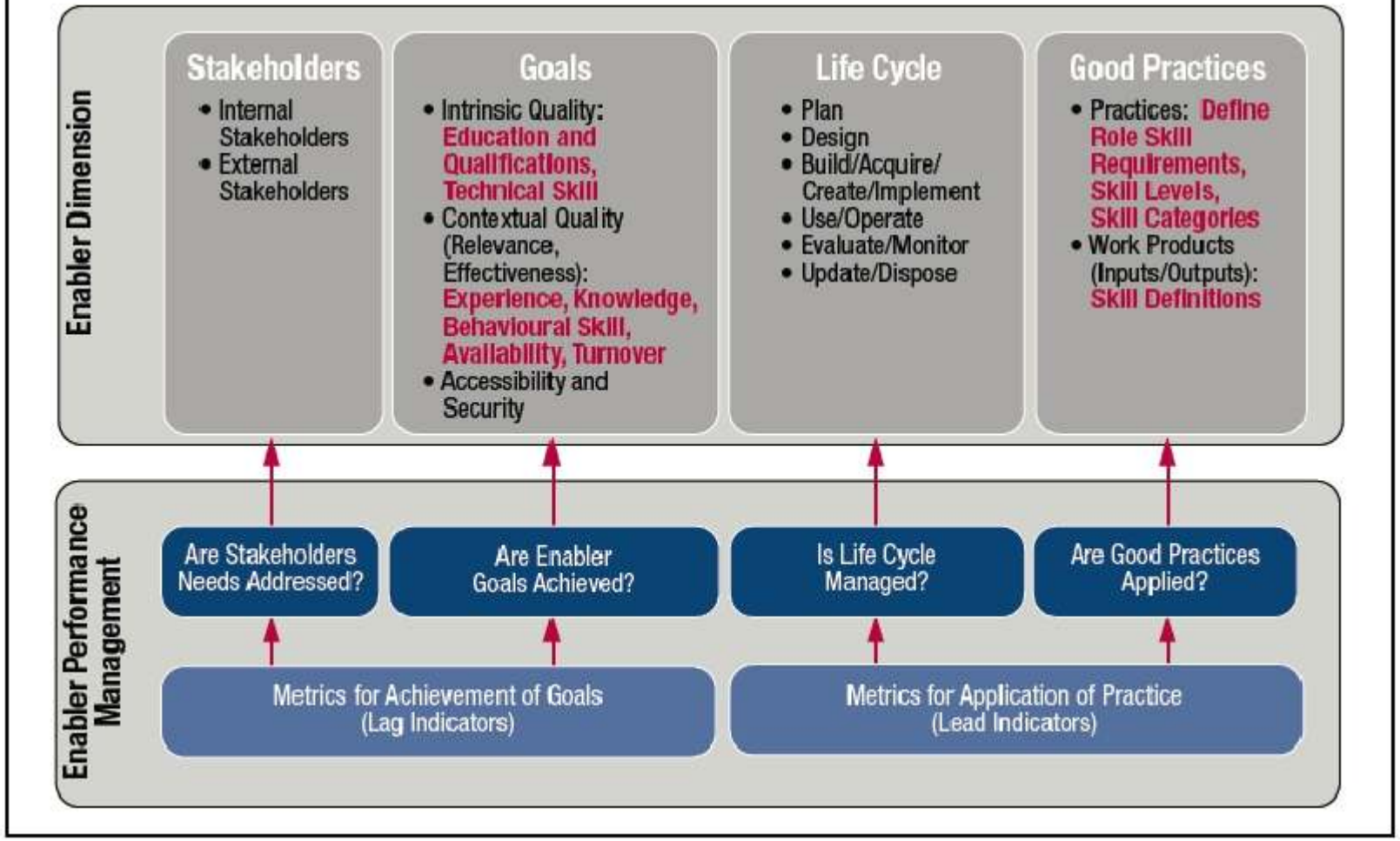
Enabler 6:
Services, Infrastructure & Applications

- RelationshipTo other Enablers

  - ✓**Information- is a service capability that is leveraged through processes to deliver internal and external services.**
  - ✓Cultural and behavioral aspects – relevant when a service-oriented culture needs to be built
  - ✓Process inputs and outputs- Most of the inputs and outputs (work products) of the process management practices and activities in the PRM include service capabilities.

Enabler 7: People, Skills and Competencies

Figure 38—COBIT 5 Enabler: People, Skills and Competencies



Enabler 7:
People, Skills and Competencies

- Identify the good practices of People, Skills and Competencies, specifically :
  - Described by different skill levels of different roles.
  - Defining Skillcategories requirements for each role.
  - Mappingskill categories to COBIT 5 process domains(APO; BAI etc)
  - These correspond to the with IT- related activities undertaken, eg. Businessanalysis, information management etc.
  - Using external sources for good practices
  - There exist in frameworks such as ITIL 3; which contains extensive guidance on how to design and operate services.
  - Consideralso TOGAF (www.opengroup.org/togaf) which provides an integrated information infrastructure reference model.

Do you have any

Questions?

COBIT 4.1
Differences to COBIT 5.0

Transition Message

- COBIT 4.1,Val IT and Risk IT users who are already engaged in governance of enterprise IT (GEIT) implementation activities can transition to COBIT 5 and **benefit from the latest and improved guidance** that it provides **during the next iterations of their enterprise's improvement life cycle** .

- COBIT 5 builds on previous versions of COBIT (and Val IT and Risk IT) and so enterprises can also build on what they have developed using earlier versions.

Areas of Change

- The following slides summaries the major changes in COBIT content and how they may impact GEIT implementation/improvement:
  1. New GEIT Principles
  2. Increase Focus on Enablers
  3. New Process Reference Model
  4. New and Modified processes separating Governance from Management
  5. Practices andActivities
  6. Revised and Expanded Goals and Metrics
  7. Inputs and Outputs provided at Management verse process level in COBIT4.1
  8. Expanded RACI charts at management process
  9. New process Capability Maturity Model.

Goals Cascade

- The goals cascaded is not ‘new’ to COBIT.
  - It was introduced in COBIT 4.0 in 2005.
- Those COBIT users who have applied the thinking to their enterprises have found value, but not everyone has recognized this value.
- The goals cascaded supports the COBIT 5 stakeholder needs principle that is fundamental to COBIT and has therefore been made prominent early in the COBIT 5 guidance.
- The goals cascaded has been revisited and updated for the COBIT 5 release.

Governance and Management Defined

- What sort of framework is COBIT ?
  - An IT audit and control framework?
    - COBIT(1996)and COBIT 2nd Edition(1998)
    - Focus on Control Objectives
  - An IT management framework?
    - COBIT 3rd Edition(2000)
    - Management guidelines added.
  - An IT governance framework?
    - COBIT 4.0 (2005) and COBIT 4.1 (2007)
    - Governance and compliances process added
    - Assurance processes removed

1. New GEIT Principles

- Val IT and Risk IT frameworks are principles-based.
- Feedback indicated that principles are easy to understand and put into an enterprise context, allowing value to be divided from the supporting guidance more effectively.
- ISO/IEC 38500 also incorporates principles to underpin its messages to achieve the same market benefit delivery, although the principles in this standard and COBIT 5 are not the same.

2. Increased Focus on Enablers

- COBIT 4.1 did not have enablers? Yes it did they were not called enablers, but they were there, explicitly or implicitly!

  Information, infrastructure, applications(services) and people (people, skills and competencies) were COBIT 4.1 resources.

  Principles, policies and frameworks were mentioned in a few COBIT 4.1 processes.

  Processes were central to COBIT 4.1 use.

  Organizational structure was implied through the responsible, accountable, consulted or informed (RACI) roles and their definitions.

  Culture, ethics and behavior were mentioned in few COBIT 4.1 processes.

3. New Process Reference Model

- COBIT 5 is based on a revised process reference model with a new governance domain and several new and modified processes that now cover enterprise activities end to end i.e. business and IT function areas.
- COBIT 5 consolidates COBIT 4.1, Val IT and Risk IT into one framework, and has been updated to align with current best practices e.g. ITIL,TOGAF.
- The new model can be used as a guide for adjusting as necessary the enterprise's own process model (just like COBIT 4.1).

4.New and Modified Processes

- COBIT 5 introduces five new governance processes that have leveraged and improved COBIT 4.1, Val IT and Risk IT governance approaches.
- This guidenance :
  - Helps enterprise to further refine and strengthen executive management-level GEIT practices and activities.
  - Supports GEIT integration with existing enterprise governance practices and is aligned with ISO/IEC 38500.

- COBIT 5 has clarified management level processes and integrated COBIT 4.1, Val IT and Risk IT content into one process reference model.

4.New and Modified Processes

- There are several New and Modified Processes that reflect current thinking, in particular:
  - APO03 Manage enterprise architecture.
  - APO04 Manage innovation.
  - APO05 Manage portfolio.
  - APO06 Manage budget and costs.
  - APO08 Manage relationships.
  - APO13 Manage security.
  - BAI05 Manage organizational change enablement.
  - BAI08 Manage knowledge.
  - BAI09 Manage assets.
  - DSS05 Manage security service.
  - DSS06 Manage business process control.

4.New and Modified Processes

- COBIT 5 processes now cover end to end business and IT activities i.e. a full enterprise level view.
- This provides for a more holistic and complete coverage of practices reflecting the pervasive enterprise wide nature of IT use.
- It makes the involvement, responsibilities and accountabilities of business stakeholders in the use of IT more explicit and transparent.

5. Practices and Activities

- COBIT 5 governance or management practices are equivalent to the COBIT 4.1 control objectives and Val IT and Risk IT processes.
- The COBIT 5 activities are equivalent to the COBIT 4.1 control practices and Val IT and Risk IT management practices.
- COBIT 5 integrates and updates all of the previous content into one new model, making it easier for users to understand and use this material when implementing improvements.

6. Enhanced Goals and Metrics

- COBIT 5 follows the same goal and metric concepts as COBIT 4.1, Val IT and Risk IT, but these are renamed enterprise goals, IT related goals and process goals reflecting an enterprise level view.
- COBIT 5 provides a revised goals cascade based on enterprise goals driving IT related goals and then supported by critical processes.
- COBIT 5 provides examples of goals and metrics at the enterprise, process and management practice levels. This is a change to COBIT 4.1, Val IT and Risk IT, which went down one level lower.

7. Revised & Enhanced I/P & O/P

- COBIT 5 provides inputs and outputs for every management practice whereas COBIT 4.1 only provides these at the process level.
- This provides additional detailed guidance for designing processes to include essential work products and to assist with interprocess integration.

8. Expanded RACI Charts

- COBIT 5 provides RACI charts describing roles and responsibilities in a similar way to COBIT 4.1, Val IT and Risk IT.
- COBIT 5 provides a more complete, detailed and clearer range of generic business and IT role players and charts than COBIT 4.1 for each management practice, enabling better definition of role player responsibilities or level of involvement when designing and implementing processes.

9. New Process Capability Assessment Model

- COBIT 5 discontinues the COBIT 4.1, Val IT and Risk IT CMM-based capability maturity modeling approach.
- COBIT 5 will be supported by a new process capability assessment approach based on ISO-IEC 15504, and the **COBITAssessment Programme** has already been established for COBIT 4.1 as an alternative to the CMM approach. COBIT 5 will be launched soon; **a supplementary guide has been provided forATO's**
  - www.isaca.org/Knowledge-Center/cobit/Pages /COBIT-Assessment-Programme.aspx
- The COBIT 4.1, Val IT and Risk IT CMM-based approaches are **not considered compatible** with the ISO-IEC 15504 approach because the methods use different attributes and measurement scales.

9. New Process Capability Assessment Model

- The COBIT 5.0 Assessment Programme approach is considered by ISACA to be more robust, reliable and repeatable as a process capability assessment method.
- The COBIT 5.0 Assessment Programme supports:
  - Formal assessment by accredited assessors (assessor training is being developed)
  - Last rigorous self-assessments for internal gap analysis and process improvement planning.
- The COBIT 5.0 Assessment Programme, in the future will also potentially enable an enterprise to obtain an independent and certified assessment aligned to the ISO/IEC standard.

Questions ?

COBIT 5 Process Capability Model

What is a Process Assessment

- ISO/IEC 15504 identifies process assessment as an activity that can be performed as part of a process improvement initiative or as part of a capability determination approach
- The purpose of process improvement is to continually improve the enterprise's effectiveness and efficiency
- The purpose of process capability determination is to identify the strengths, weaknesses and risk of selected processes with respect to a particular specified requirement through the processes used ad their alignment with the business need
- It provides an understandable, logical, reputable, reliable and robust methodology for assessing the capability of IT processes.

Process Capability Assessment

- The COBIT Assessment Programme approach is considered by ISACA to be more robust, reliable and repeatable as a process capability assessment method.
- The COBIT Assessment Programme supports:
  - Formal assessment by accredited assessors
  - Less rigorous self-assessment for internal gap analysis and process improvement planning
- The COBIT Assessment Programme potentially enables an enterprise to obtain an independent and certified assessments aligned to the ISO/IEC standards.

The COBIT Assessment Program

- The COBIT Assessment Program includes:
  - COBIT ProcessAssessment Model (PAM) – using COBIT 4.1
  - COBIT ProcessAssessment Model (PAM) – using COBIT 5
  - COBIT Assessor's Guide - – using COBIT 4.1
  - COBIT Assessor's Guide - – using COBIT 5.0
  - COBIT Self Assessor's Guide - – using COBIT 4.1
  - COBIT Self Assessor's Guide - – using COBIT 5.0
- The COBIT Process Assessment Model (PAM) brings together two proven heavyweights in the IT arena, ISO and ISACA.
- The COBIT PAM adapts the existing COBIT 4.1 & COBIT 5.0 content into an ISO 15504 compliant process assessment model.

Process Capability Assessment

- **COBIT Process Assessment Model(PAM): Using COBIT 4.1 & COBIT 5.0**
  - Serves as a base reference document for the performanceof a capability assessment of an organization's current IT processes against COBIT
- **COBIT Assessors Guide : Using COBIT 4.1 & COBIT 5.0**
  - Providesdetails on how to undertake a full ISO-compliant assessment
- **COBIT Self-Assessment Guide : Using COBIT 4.1 & COBIT 5.0**
  - Providesguidance on how to perform a basic self-assessment against COBIT processes.

Differences Between a Capability & Maturity Assessment

- Historically most frameworks from COBIT, ITIL to PRINCE2 have adoptedthe SEI (Software Engineering Institute) CMMI approachwhich combines a Capability and A Maturity Assessmentinto a single assessment.

- ISO 15504 argues that they are two separate assessments:
  - ✓ **A Maturity Assessmentis done at an Enterpriseor Organizational level** anduses a different measurement scale than a capability assessment and different criteria and attributes.
  - ✓ **A Capability Assessmentis done at a Process Level** and is done for purpose of process improvement.You cannot 'roleup'an assessmentof many different processes mathematically to an enterprise level. It works for SEI's CMMI because they are assessing a single process, software engineering development or application development. Most frameworks like COBIT contain 34 and 37 processesrespectively for COBIT 4.1 and COBIT 5.
  - ✓ So theconcept of a Maturity Assessment has been redevelopedin COBIT 5 to theISO 15504 Process Capability Assessment

Differences to a CMM Model ?

- **But don't we already have maturity models for COBIT 4.1 processes ?**
- The new COBIT Assessment Program
  - Arobust assessment process based on ISO 15504
  - Aligns COBIT's maturity model scale with ISO 15504 standard
  - New capability based assessment model includes:
    - Specific process requirements derived from COBIT 4.1
    - Ability of processto achieve process attributes based on 15504
    - Evidencerequirements
    - Assessors qualifications and experiential requirements.
- Results in a more robust, objective and reputable assessment.
- Assessment results will likely vary from existing COBIT maturity models.
- COBIT 5 only adopts the ISO 15504approach

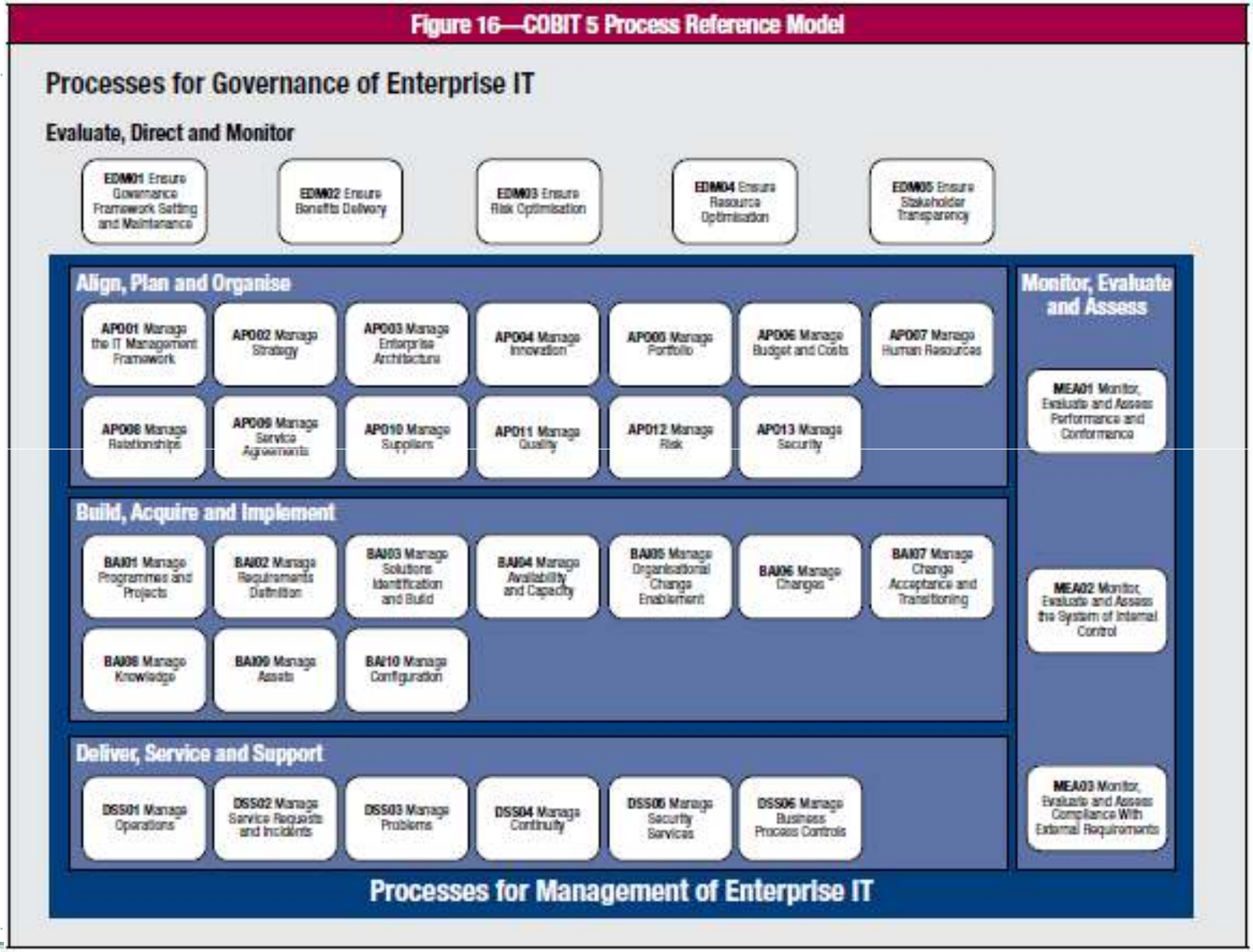
Process Capability Assessment Differences COBIT 4.1 & 5

- The key difference to note from the above definitions:
  - A Maturity Assessment is done at an Enterprise organizational level and uses a different measurement scale than a capability Assessment different criteria and attributes.
  - A Capability Assessment is done at a process level and is done for purposes of process improvement

Advantages of the ISO 15504 Approach

- A robust assessment process based on ISO 15504
- An alignment of COBIT's maturity model scale with the internal standard
- A new capability-based assessment model which includes:
  - Specific process requirements derived from COBIT 4.1 & COBIT 5
  - Ability to achieve process attributes based on ISO 15504
  - Evidence requirements
- Assessors qualifications and experiential requirements
- Results in a more robust, objective and reputable assessment.

COBIT 5 Process Reference Model



The Process Assessment Model (PAM) Explained

PAM Scope

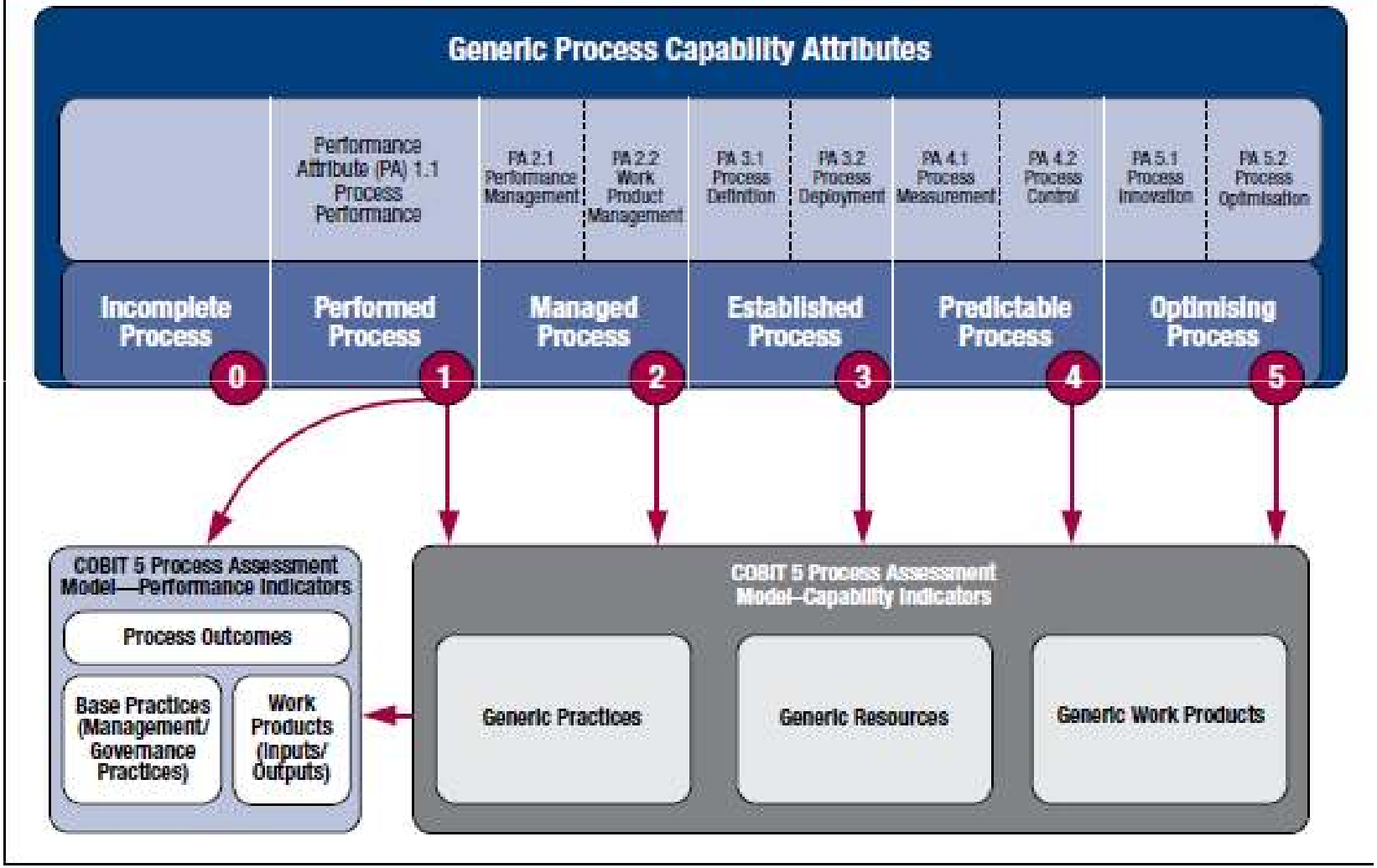
- AProcess Assessment Model is related to one more Process Reference Models. It forms the basis for the collection of evidence and rating of process capability. A Process Assessment Model shall relate to at least one process from the specified Process Reference Model(s).

- AProcess Assessment Model shall address, for a given process, all, or a continuous subset of the levels(starting at level 1) of the measurement framework for process capability for each of the processes within its scope.

- Note It would be permissible for a model, for example, to address solely level1, or to address levels 1,2 and 3, but it would not be permissible to address levels 2 and 3 without level 1.

Summary of Process Capability Model

Figure 19—Summary of the COBIT 5 Process Capability Model



The Capability Levels

- Level 0, Incompleteprocess—The process is not implemented or fails to achieve its processpurpose.At this level, there is little or no evidence of any systematic achievement of the process purpose.
- Level 1, Performed process (one attribute)—The implemented process achieves its processpurpose.
- Level 2, Managed process (two attributes)—The previously described performed processis nowimplemented in a managed fashion (planned,monitored and adjusted)and its work productsare appropriately established,controlled and maintained.
- Level 3, Established process (two attributes)—The previouslydescribed managed processis nowimplemented using a defined process that is capable of achieving its processoutcomes.
- Level 4, Predictable process (two attributes)—The previously described established processnow operates within defined limits to achieve its process outcomes.
- Level 5, Optimizing process (two attributes)—The previously described predictable processis continuouslyimproved to meet relevant current and projected business goals.

The Capability Levels

Each capability level can be achieved only when the level below has been fully achieved. For example, a process capability level 3 (established process) requires the process definition and process deployment attributes to be largely achieved, on top of full achievement of theattributes for a process capability level 2 (managed process).

There is a significant distinctionbetween process capability level 1 and the higher capability levels. Process capability level 1 achievement requires the process performance attributeto be largely achieved, which actually means that the process is being successfully performed and the required outcomes obtained by the enterprise. The higher capability levels then add different attributesto it.

Mapping to PRM's

- A Process Assessment Model shall provide an explicit mapping from the relevant elements of the model to the relevant process attributes of the measurement framework.

- The mapping shall be complete, clear and unambiguous. The mapping of the indicators within the Process Assessment Model shall be:

  - ✓ The purpose and outcomes of the processes in the specified Process Reference Model
  - ✓ The process attributes (including all of theresults of achievements listedfor each process attribute) in the measurement framework.
  - ✓ This enables ProcessAssessment Models that are structurally different to be related to the same Process Reference Model.

Measurement Framework

- ✓ COBIT Assessment Process measures the extent to which a given process achieves specific attributes relative to that process –
- ✓ COBITAssessment Process defines 9 Process Attributes (based on ISO/IEC 15504-2)
  - PA1.1- process performance
  - PA2.1- work product management
  - PA2.2- performance management
  - PA3.1- process definition
  - PA4.1- process deployment
  - PA4.2- process control
  - PA5.1- process innovation
  - PA5.2- continuous optimization

Process Attributes Rating Scale

- COBITAssessment Process measures the extent to which a given process achieves the “Process Attributes”

N, Not achieved - 0 to 15%achievement

There is little or no evidence of achievement of thedefined attributes in the assessedprocess

P, Partially achieved - >15 to 50% achievement

There is someevidence of an approach to and someachievement of the defined attributes in the assessed process. Someaspects of achievement of theattribute may be unpredictable.

L, Largely achieved - >50to 85% achievement

There is evidence of a systematic approach to and significant achievement ofthe defined attributes in the assessed process.Some weakness related to this attribute may be exist in the process.

F, Fully achieved - >85to 100%achievement

There is evidence of a complete& systematic approachto and full achievement of the defined attributes in the assessed process.No significant weakness related to this attribute exist in the assessed process.

Assessor Assessment Steps

Assessment ProcessActivities

- Initiation
- Planning theAssessment
- Briefing
- Data Collection
- DataValidation
- ProcessAttribute Rating
- Reporting the Results

1: Initiation

Identify thesponsor and define the purpose of theassessment

-why it is being carried out.

Define the scope of the assessment

-which processes are being assessed

-what constraints ,if any, apply to the assessment

Identify any additionalinformation that needs to be gathered

Select theassessment participants, theassessment team and define the roles of team members

Define assessment inputs and outputs . Have them approved by the sponsor

2: Planning the Assessment

An assessment plan describing all activities performed in conducting the assessment is

- developed and
- documented together with
- an assessment schedule

- Identify theproject scope
- Securethe necessary resources to perform the assessment
- Determine the method of colleting, reviewing ,validating and documenting theinformation required for the assessment
- Co-ordinateassessment activities with the organizational unit being assessed

3: Briefing

- The assessment Team Leader ensures that the assessment team understands theassessment
  - input
  - process and
  - output
- Brief the Organizational Unit on the performance of the assessment
  - PAM, assessment scope ,scheduling ,constraints,roles and responsibilities,

    resource requirements ,etc

4: Data Collection

- The assessor obtains (and documents) an understanding of the process(es) includingprocess purpose ,inputs,outputs and work products, sufficient to enableand support the assessment
- Datarequired for evaluating the processes within the scope of the assessment is collected in a systematic manner
- The strategy and techniques for theselection ,collection ,analysis of data and justificationof the ratings are explicitly identified and demonstrable
- Each process identified in the assessment scope is assessed on the basis of objective evidence.
  - The objective evidence gathered for each attribute of each process assessedmust be sufficient to meet the assessment purpose and scope
  - Objective evidence that supports the assessors judgment of process attribute rating is recorded and maintained in the assessment record.
    - This recordprovides evidence to substantiate the ratings and to verify compliance with the requirements.

5: Data Validation

- Actions are taken to ensure that the data is accurate and sufficiently covers the assessment scope, including
  - Seekinginformation from first hand ,independent sources
  - Using past assessment results ; and
  - Holding feedback sessions to validate the information collected.
- Some data validation may occur as the data being collected

6: Process Attribute Rating

- Foreach process assessed , a rating is assigned for each process attributeup toand includingthe highest capability level defined in the assessment scope
- The rating is based on data validated in the previous activity
- Traceability shall be maintained between the objective evidence collected and the process attributeratings assigned
- Foreach process attribute rated , the relationshipbetween theindicators and the objective evidence is recorded.

7: Reporting the Results

- The results of the assessment are analyzed and presented in a report
- The report also covers any key issues raised during theassessment such as:
- Observed areas of strength and weakness
- Findingsof high risk
  - i.e. magnitude of gap between assessed capability and desired/required capability

Assessor Certification

- COBIT process Assessment roles:

  - Lead Assessor-a “competent ”assessor responsible for overseeing the assessment activities

  -Assessor- an individual ,developing assessor competencies , that performs the assessment activities

- Assessor Competencies:

  -Knowledge ,skills and Experience

  - With the process Reference Model ; ProcessAssessment Model , methodsand tools;
    andrating processes
  - With the processes/domainsbeing assessed
  - Personalattributes which contribute to effective performance

- An assessor’s training and certificate course for assessors is being developed for COBIT 4.1 and COBIT 5.0Availability Q1 2013

Questions?

That's All

Thanks for being together