FRAMEWORK AND GOVERNANCE

Asst. Prof. Kemathat Vibhatavanij Ph.D.

Governance

Corporate Governance (Business Dictionary)

- The framework of **rules and practices** by which **a board of directors *ensures* accountability, fairness, and transparency** in a company's relationship with its all stakeholders

From ISACA (Information Systems Audit and Control Association)

- the **set of responsibilities and practices** exercised by **the board and Executive management** with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly

IT Governance

From ISACA (Information Systems Audit and Control Association)

- an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT1 sustains and extends the organization's strategies and objectives

From ITGI (IT Governance Inst.)

- The framework for the leadership, organizational structures and business processes, standard and compliance to these standards, which ensures that the organization's information systems support and enable the achievement of its strategies and objectives

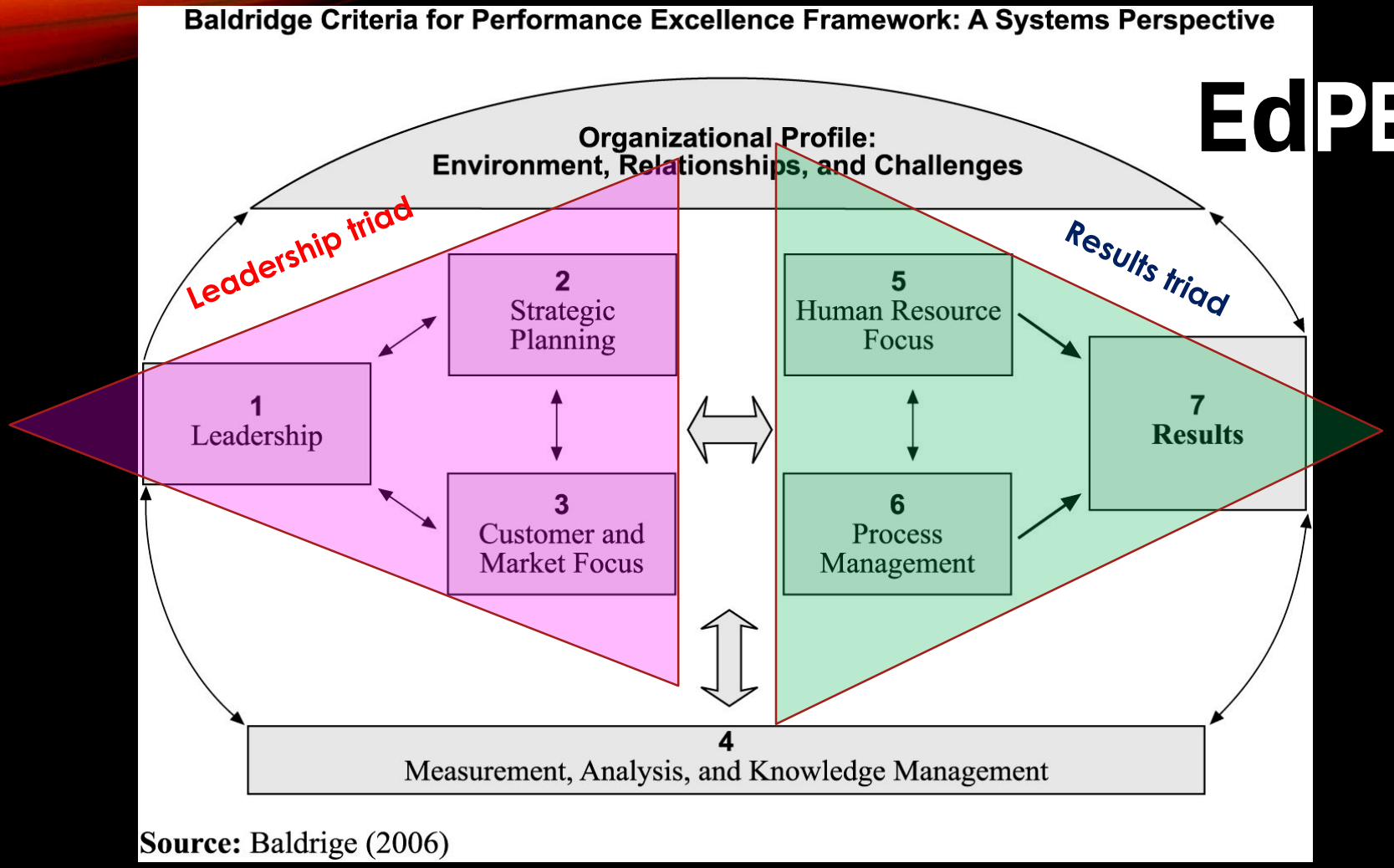
Information security governance

an integral and transparent part of enterprise governance and be aligned with the IT governance framework

Management

Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives

EdPEx


Baldridge Criteria for Performance Excellence Framework: A Systems Perspective
Organizational Profile:
Environment, Relationships, and Challenges
Leadership triad
Results triad
1
Leadership
2
Strategic
Planning
3
Customer and
Market Focus
5
Human Resource
Focus
6
Process
Management
7
Results
4
Measurement, Analysis, and Knowledge Management
Source: Baldrige (2006)

ORGANIZATIONAL PROFILE

Organizational Description_1

Organizational Environment

- The business (e.g. Educational Program and Service offering: mechanism to deliver EduProgAndServ)
- Vision and mission
- Workforce profile (faculty/staff gr./seg., workforce engagement, educational requirement, workforce and job diversity, health and safety requirement)
- Asset (facilities, tech. and equipment)
- Regulatory requirements (health & safety regulations, accreditation, cert., EduIndStd.,financial, environmental, program and service regulations)

Organizational Description_2

Organizational Relationships

- Organizational structure (Org. structure, reporting relationships: Governance board, senior leaders, parent org. etc.)
- Customers and stakeholders (students, parents, alumni, merchandizer)
  - Key market segment
  - Service expectation (program, people), CEM, CRM
  - CSR (corporate social relationship)
- Suppliers and Partners
  - Roles of those supplier, partners and collaborators to enhance OUR competitiveness
  - Mechanism for communicating
  - Implementing innovation

Organizational situation

Competitive environment

- Competitive position
- Competitiveness changes
- Comparative data

Strategic context

Performance improvement system

Leadership triad

Leadership

Senior leadership

- Vision, value, mission
- Comm. and org. perf.

Governance and societal responsibility

- Org. governance
- Legal and ethical behavior
- Societal resp. and supp. of key communities

Strategic planning

Strategy development

- Strategy development process
- Strategic objective

Strategy implementation

- Action plan development and deployment
- Performance projection

Customer focus

VOC/VOS

- Listening to customer (students)
- Determination of customer satisfaction and engagement

Customer engagement

- Program and service offering and customer support
- Building relationships with customer (students)

Results triad

Workforce Focus

Workforce environment

- Workforce capability and capacity
- Workforce climate

Workforce engagement

- Workforce performance
- Assessment of workforce engagement
- workforce and leader development

Operations Focus

Work process

- Program, service and process design
- Process management

Operational effectiveness

- Cost control
- Supply-chain management
- Safety and emergency preparedness
- innovation management

Results

Student learning and process result

Customer focus result

Workforce focus result

Leadership and governance result

Budgetary, financial and market result

IT Governance

Objectives

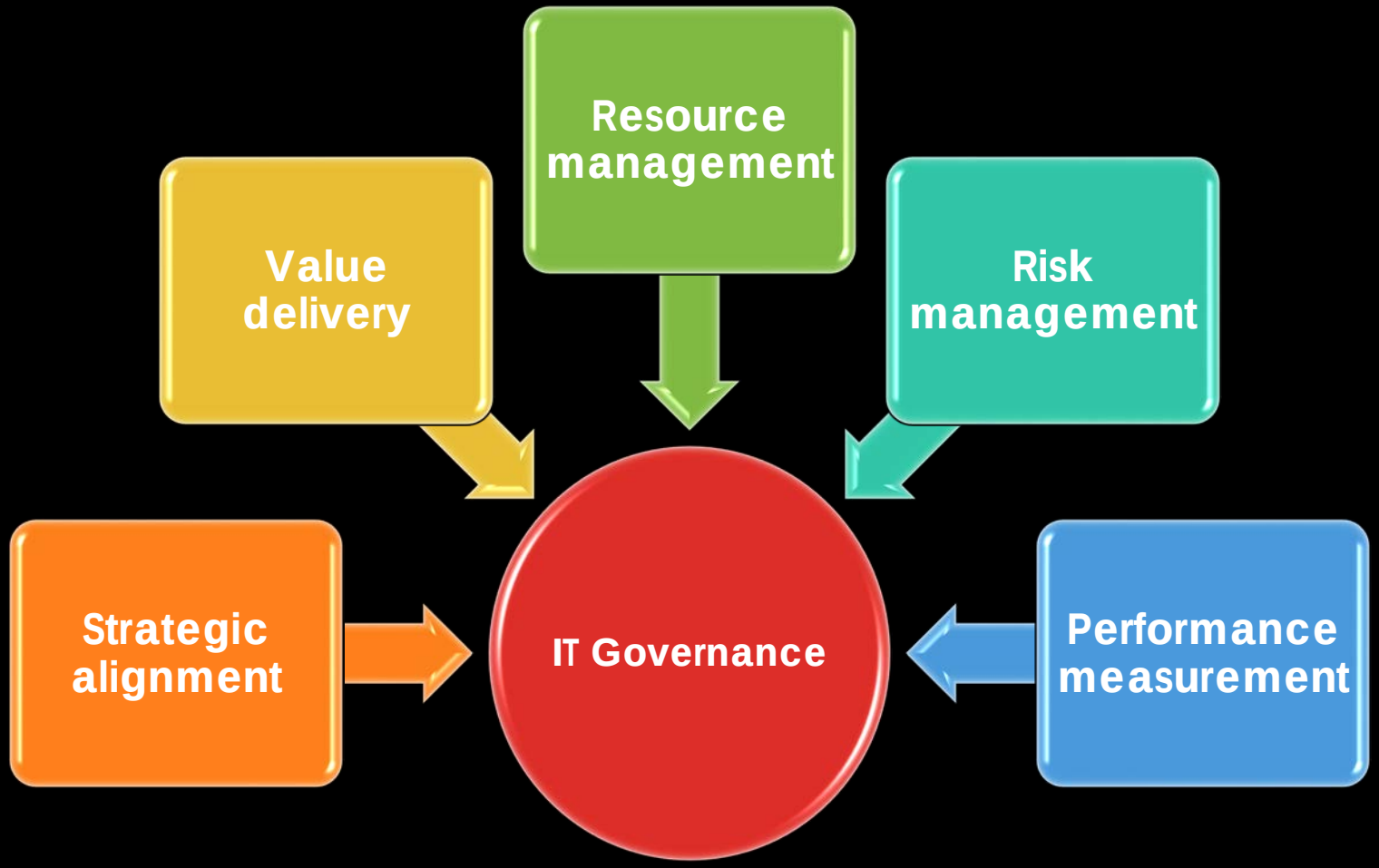
- Align with business
- Enable business and maximize benefit
- Resources are used responsibly
- Risk are managed appropriately

Driver

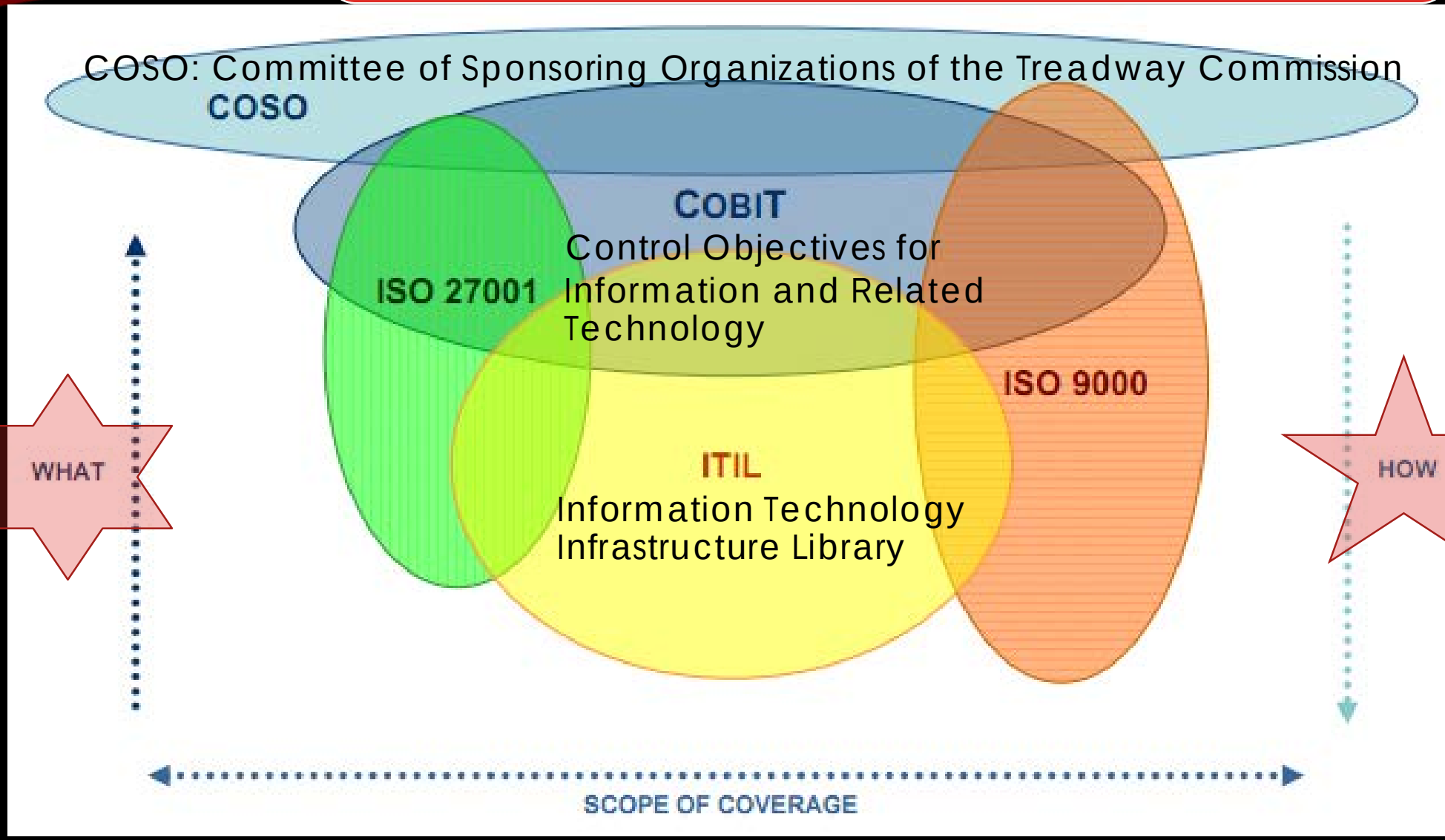
- Legal issues, for instance, Turnbull Guidance, Sarbanes-Oxley, BIS, Basel 2
- Org. risk in the increasing intellectual capital value
- To align tech. projects with strategic org. goals
- The proliferation of threats to information
- Compliance requirement

BIS (Bank of Int'l Settlements)

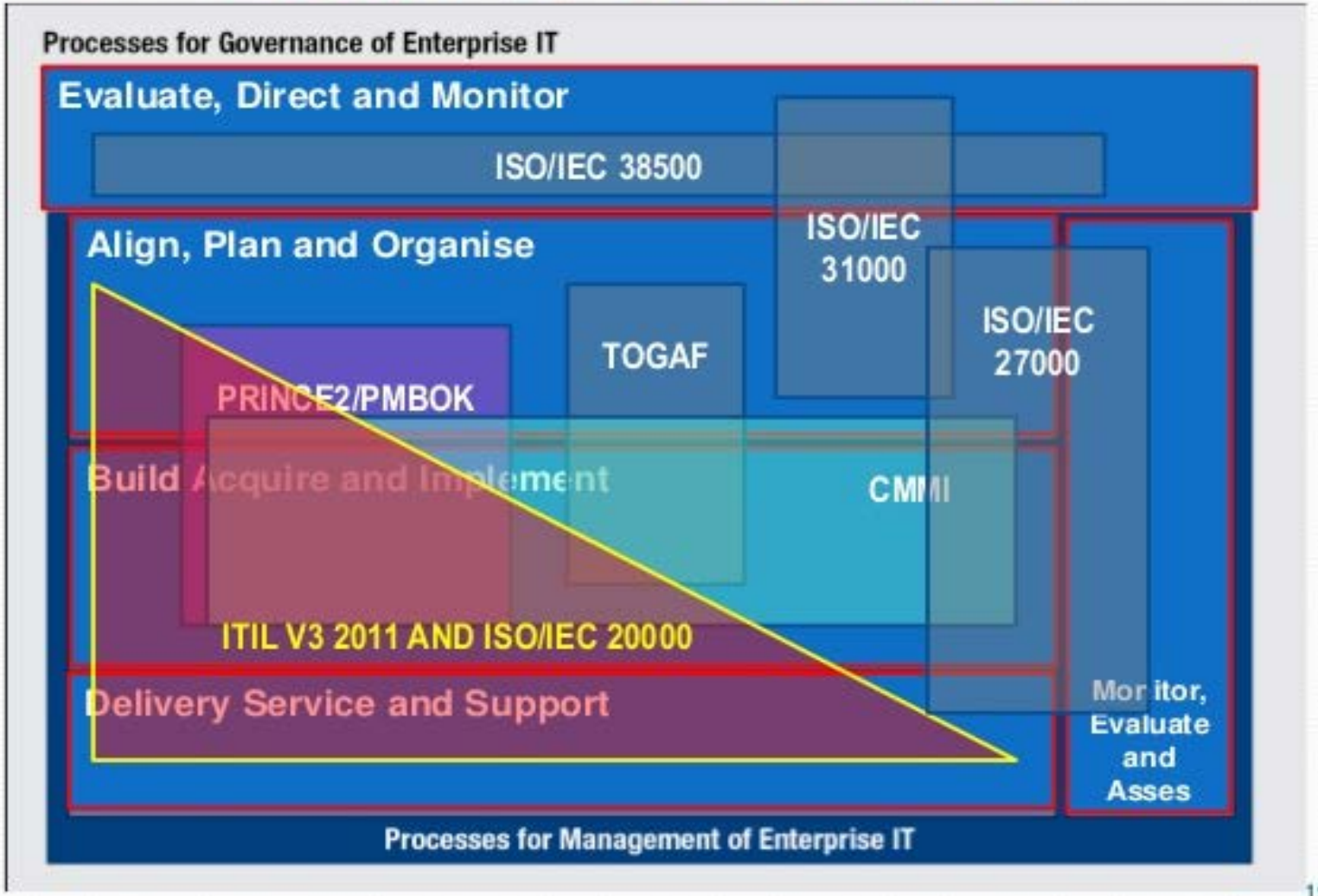
IT Governance Focus Areas



IT related frameworks



COBIT 5: COVERAGE



Focus Areas

Strategic alignment

- Focuses on ***ensuring the linkage of business and IT plans***; defining, maintaining and validating the IT value proposition; and align IT operations with enterprise operations

Value delivery

- Is about executing the value proposition throughout the delivery cycle, ***ensuring that IT delivers the promised benefits against the strategy***, concentrating on optimizing cost and proving the intrinsic value of IT

Resource management

- Is about the ***optimal investment in, and the proper management of, critical IT resources***: applications, information, infrastructure and people. Key issue relate to the optimization of knowledge and infrastructure

Focus Areas

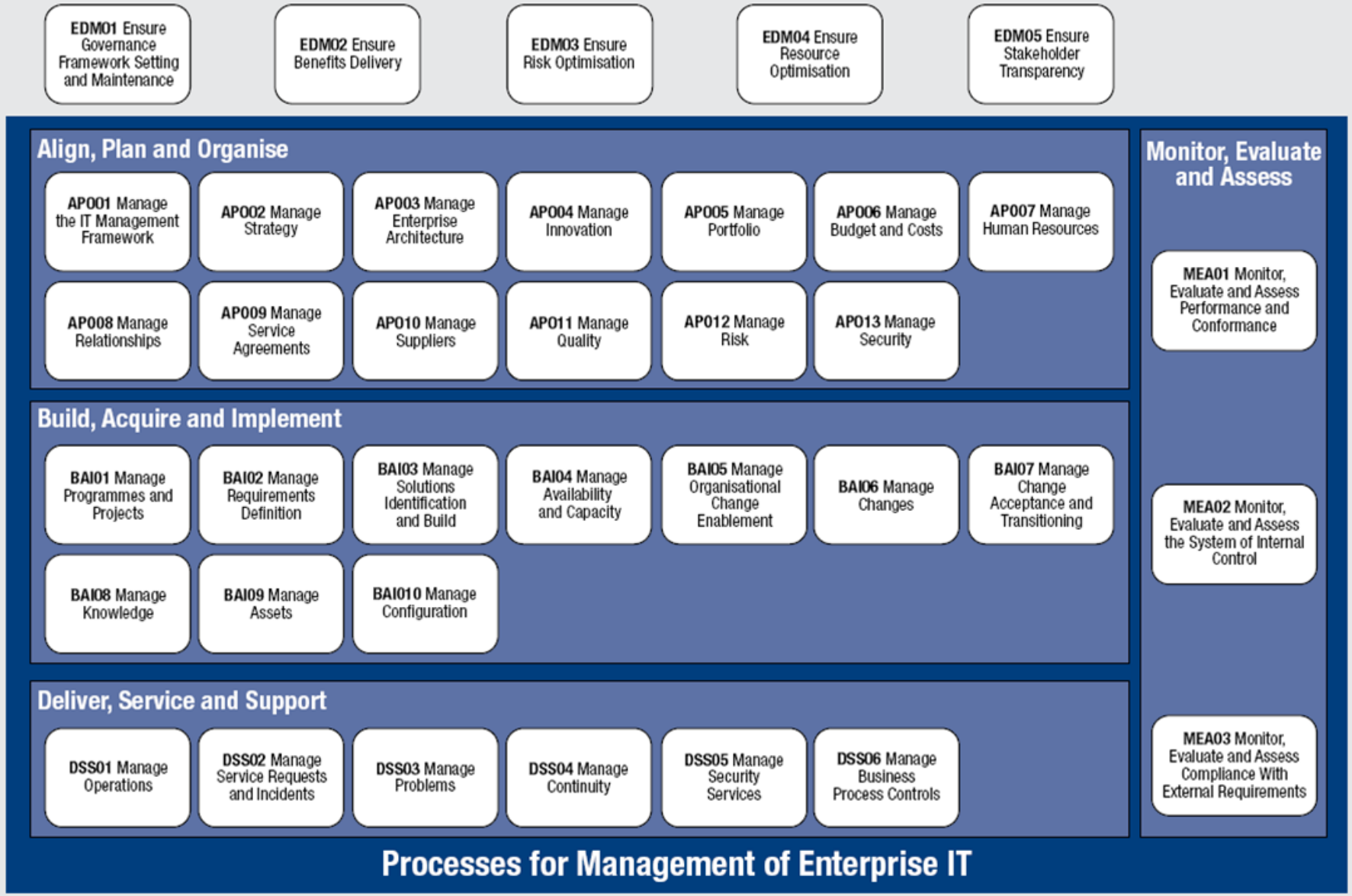
Risk management

- Requires ***risk awareness by senior corporate officers***, ***a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements***, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organization

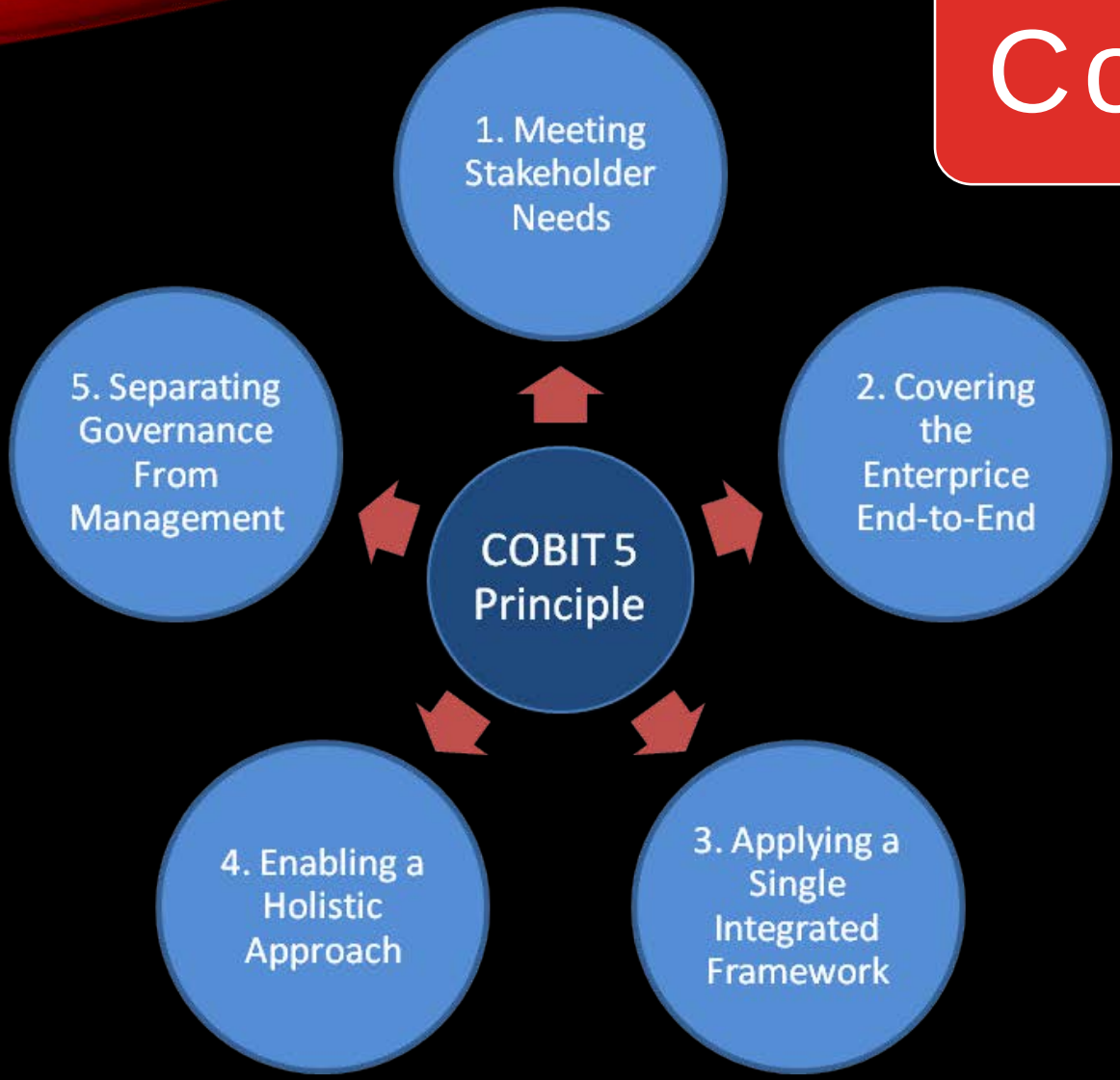
Performance measurement

- **Tracks and monitors** strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting

Processes for Governance of Enterprise IT



CoBIT 5 Principles



Meeting stakeholder needs

Enterprises exists to create value for their stakeholders by maintaining a **balance** between the realization of ***benefits*** and the ***optimization of risk*** and ***use of resources***

For whom are the benefits?
Who bears the risk?
What resources are required?

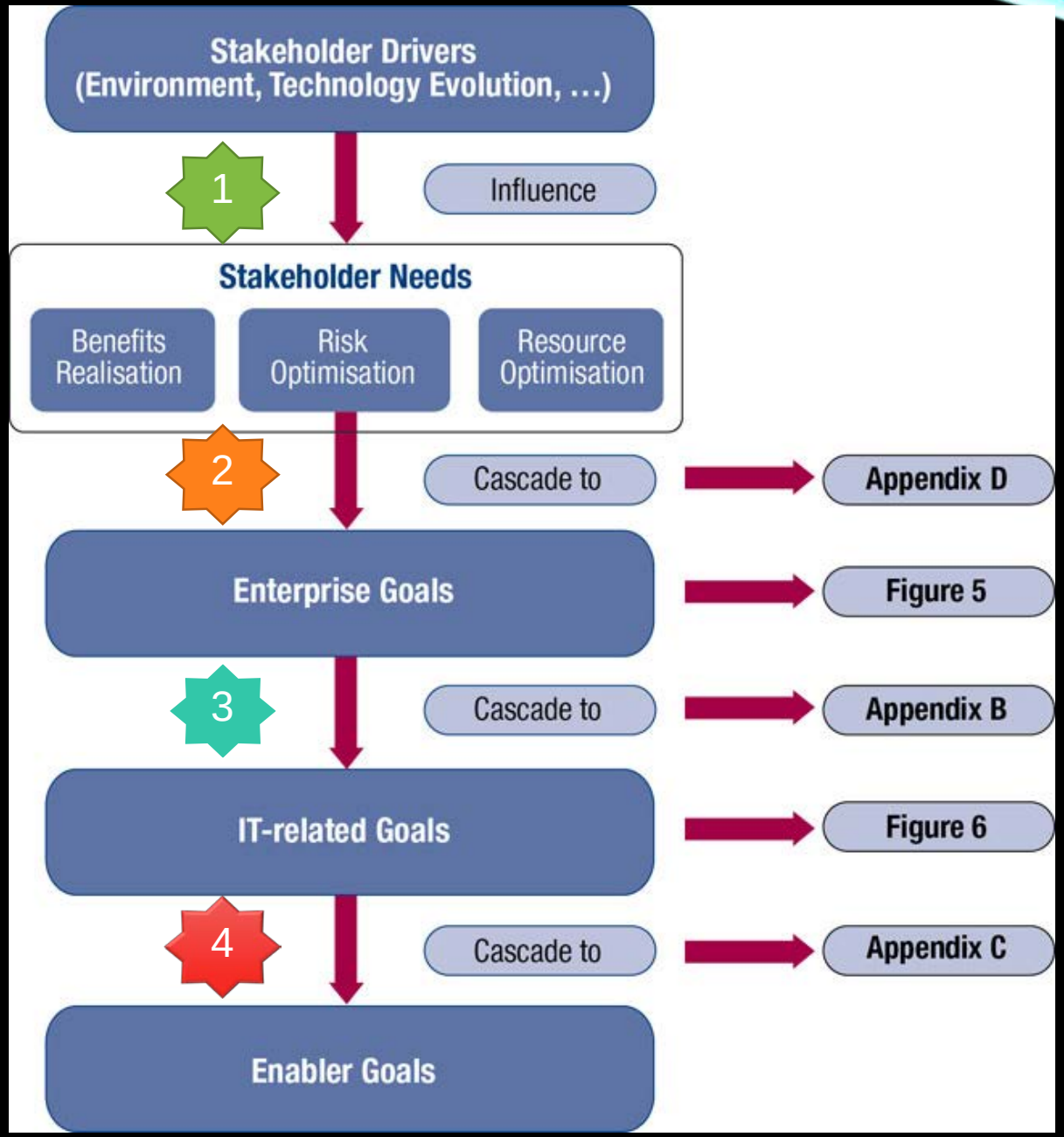
Internal Stakeholders	Internal Stakeholder Questions
• Board • CEO • Chief financial officer (CFO) • CIO • Chief risk officer (CRO) • Business executives • Business process owners • Business managers • Risk managers • Security managers • Service managers • Human resource (HR) managers • Internal audit • 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 concrete vital primary business processes are dependent on IT, and what are the requirements of business processes? • What has been the average overrun of the IT operational budgets? How often and how much do IT projects go over budget? • How much of the IT effort goes to fighting fires rather than to enabling business improvements? • Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives? • How long does it take to make major IT decisions? • Are the total IT effort and investments transparent? • Does IT support the enterprise in complying with regulations and service levels? How do I know whether I am compliant with all applicable regulations?
External Stakeholders	**External Stakeholder Questions**
• Business partners • Suppliers • Shareholders • Regulators/government • External users • Customers • Standardisation organisations • External auditors • Consultants • Etc.	• How do I know my business partner's operations are secure and reliable? • How do I know the enterprise is compliant with applicable rules and regulations? • How do I know the enterprise is maintaining an effective system of internal control? • Do business partners have the information chain between them under control?

Internal and External Stakeholders

Goal Cascade

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

1. Stakeholder drivers influence stakeholder needs
2. Stakeholder needs cascade to *enterprise goals*
3. Enterprise goals cascade to *IT-related goals*
4. IT-related goals cascade to enabler goals



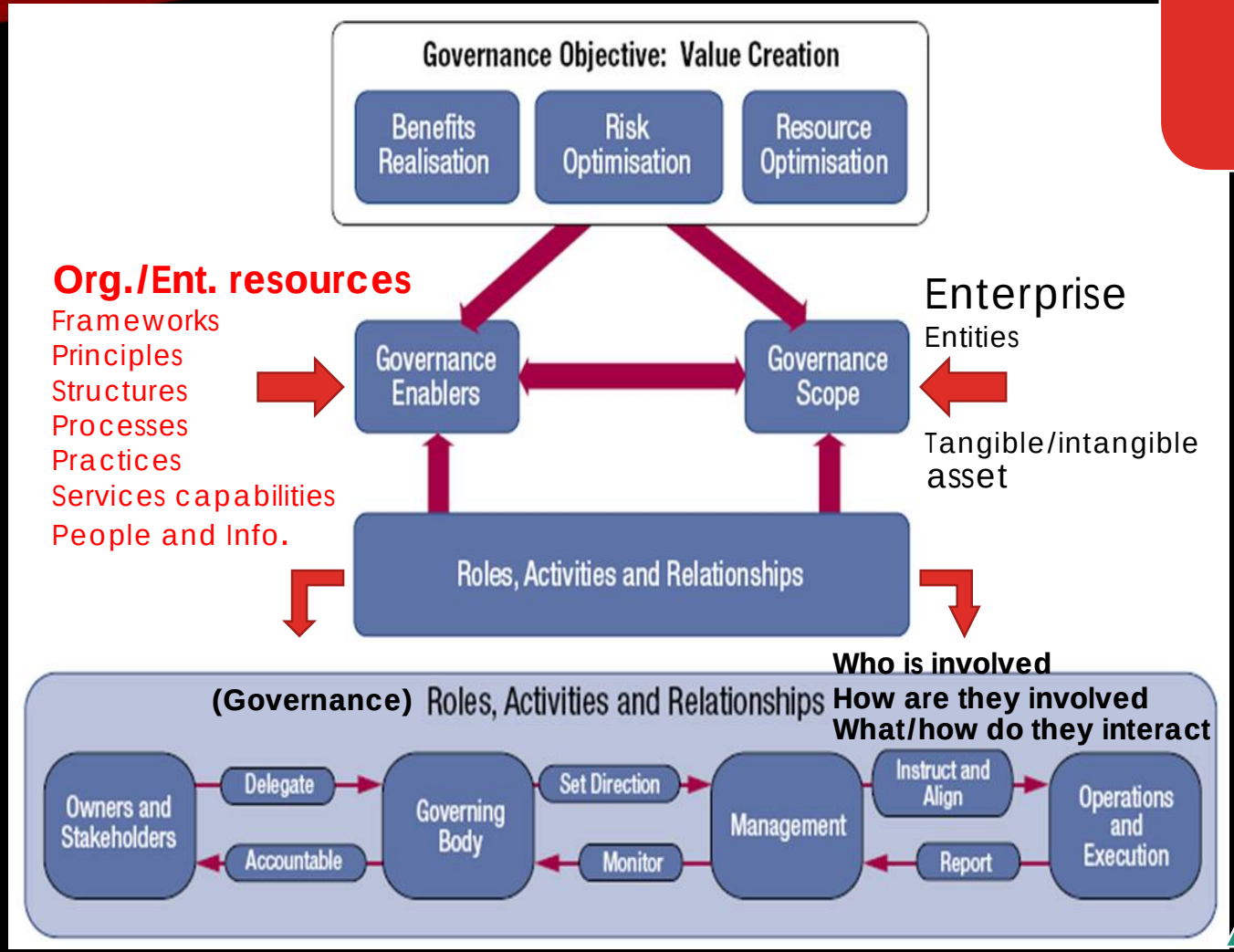
MEETING STAKEHOLDER NEEDS

Figure 4—COBIT 5 Enterprise Goals

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

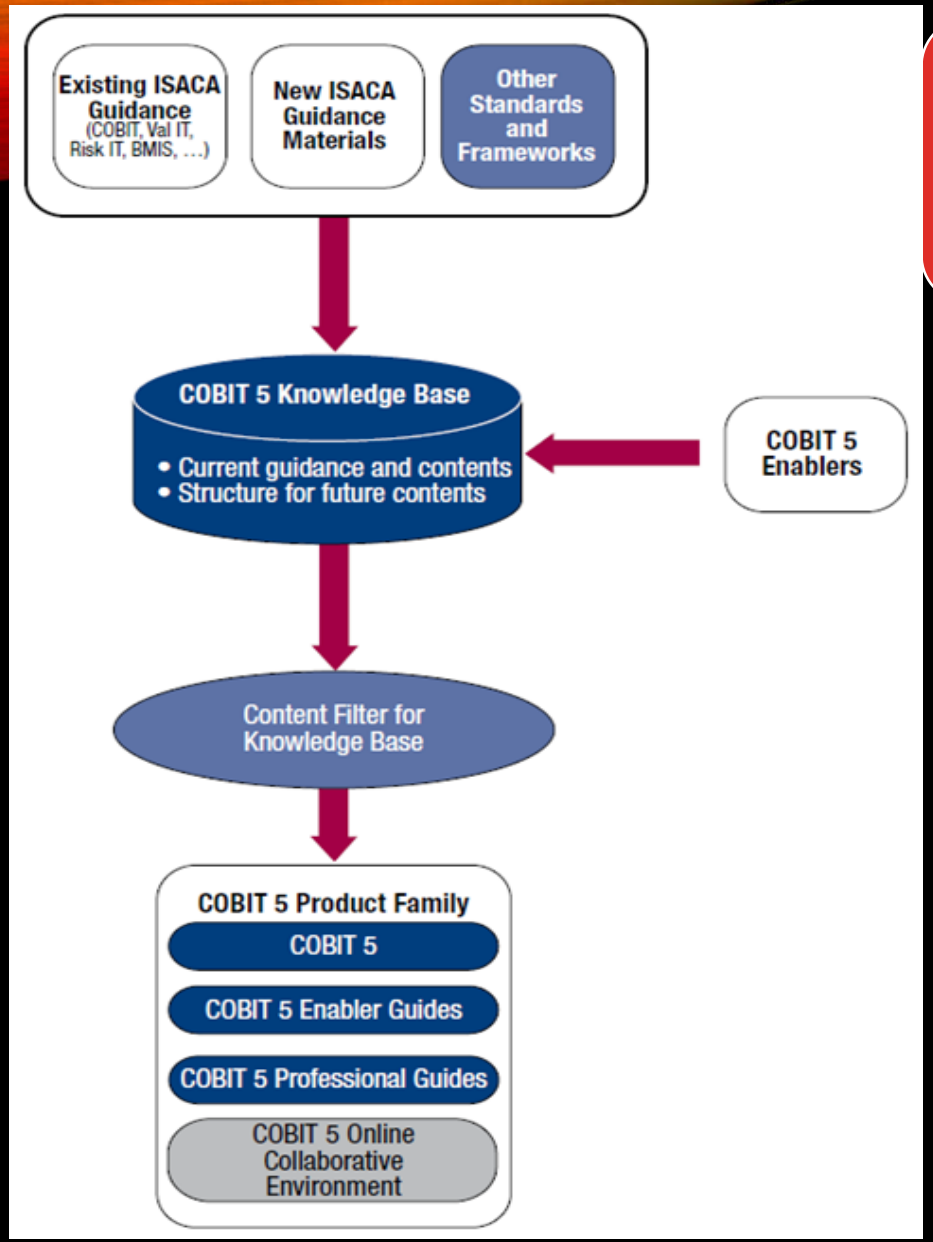
IT BSC Dimension	Information and Related Technology Goal	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business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

Covering the enterprise end-to-end



Integrate governance of enterprise IT into enterprise governance.

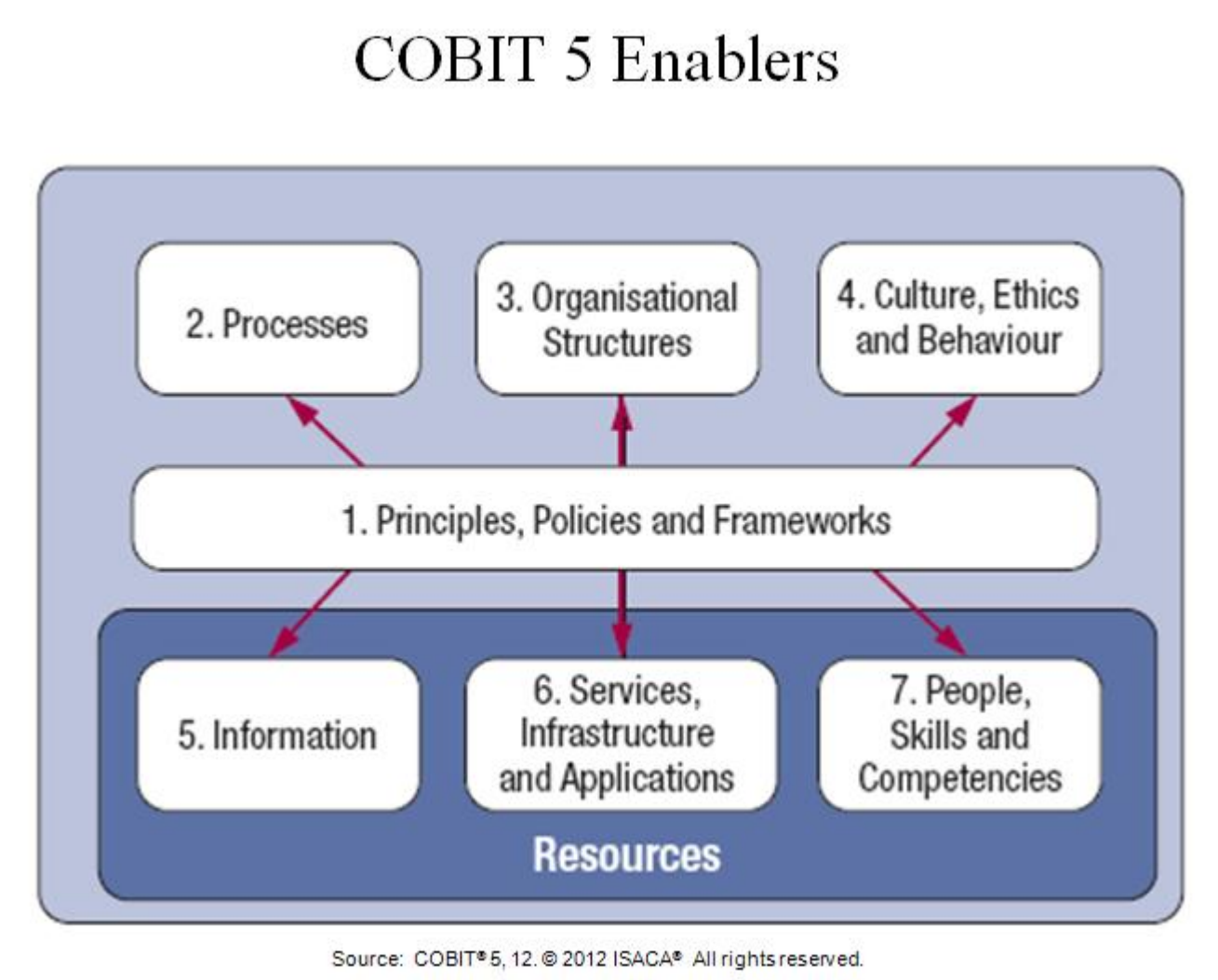
Cover all functions and processes required to govern and manage enterprise information and related technology.



Applying a single integrated framework

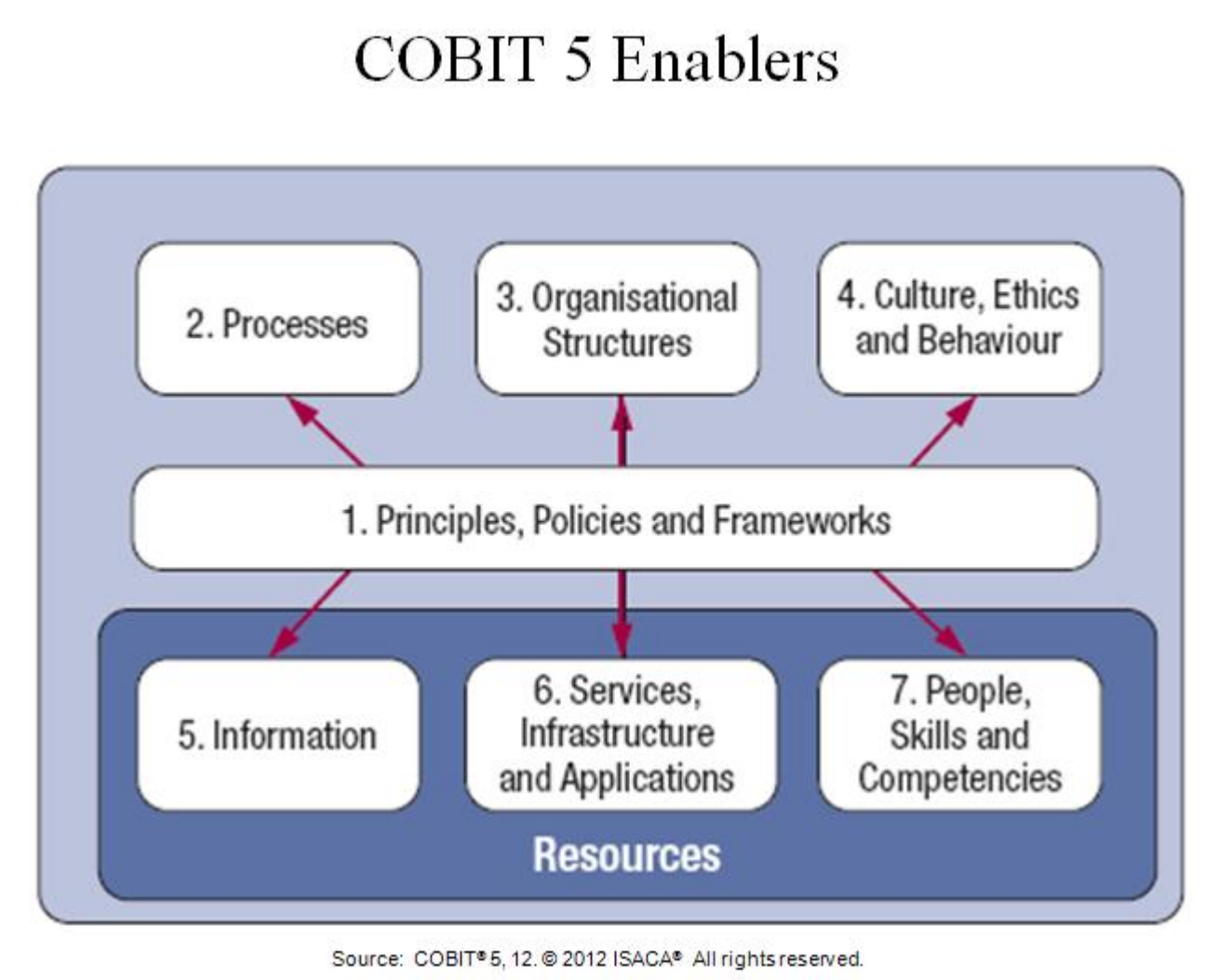
1. Align with other latest relevant standards and frameworks
2. Enterprise coverage (integrate effectively with other frameworks, standards and practices)
3. Simple architecture for structuring guidance materials and producing a consistent product set
4. Integrated all knowledge that belong to ISACA frameworks

Enabling a Holistic Approach



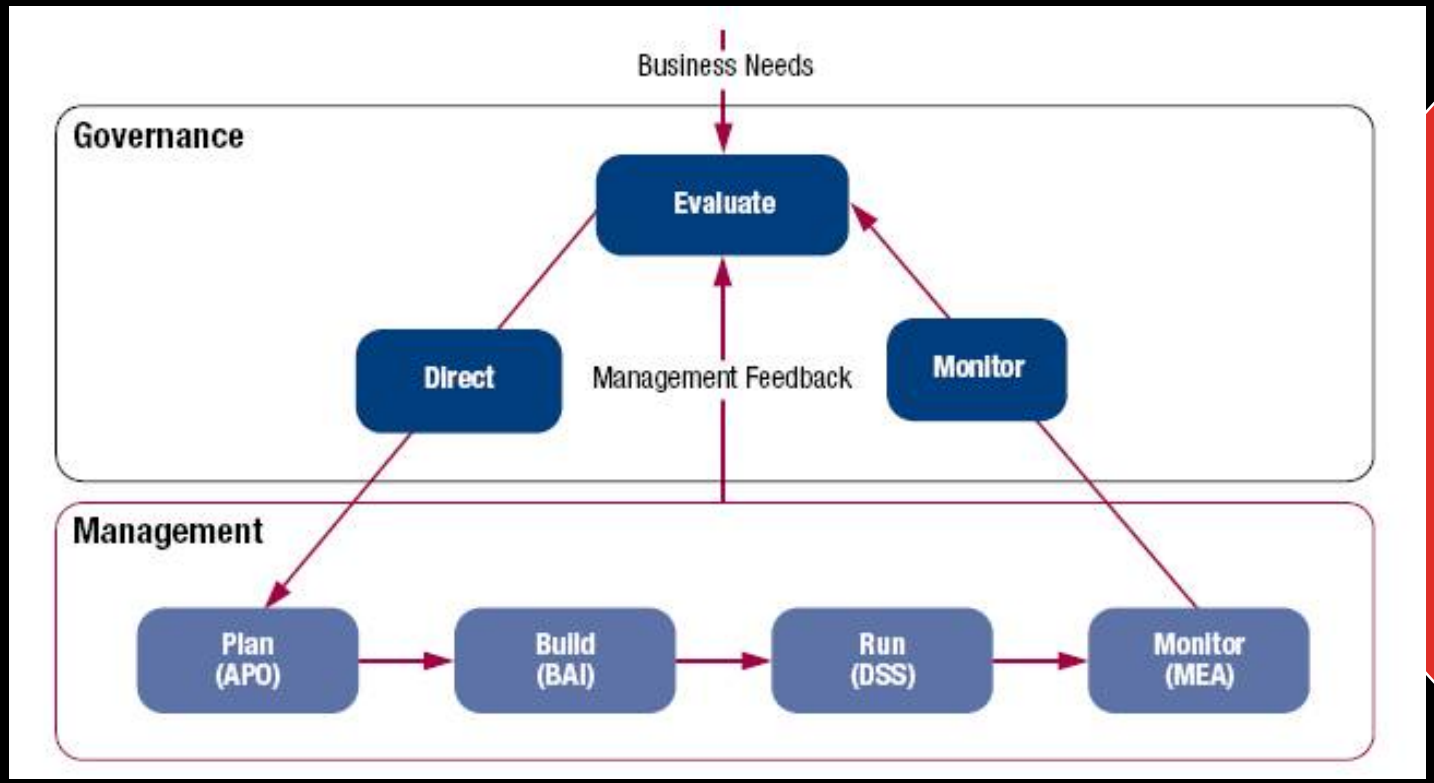
- PPF: translate the desired behavior into practical guidance for day-to-day management
- P: set of practices and activities to achieve certain objective and produce a set of outputs
- OS: key decision-making entities in an enterprise

Enabling a Holistic Approach



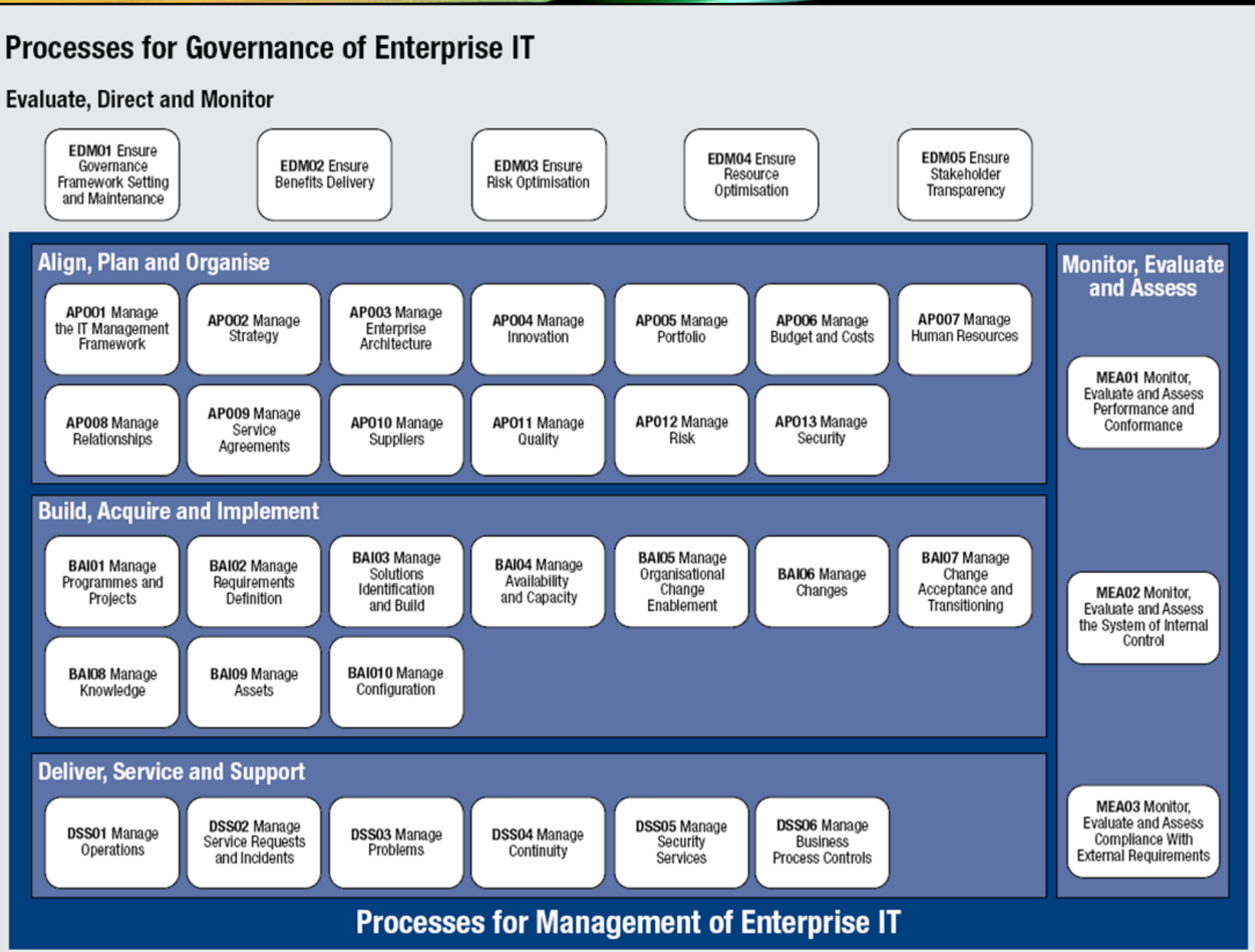
- CEB: success factors in governance and management activities
- I: keeping the organization running and well governed
- SIA: IT processing and services
- PSC: the success of all activities for making correct decision and taking corrective actions

Separating Governance from Management



Make a **clear distinction** between **governance** and **management**

COBIT5 PROCESS REFERENCE MODEL



END OF LECTURE 2