COBIT 5 Used in a Security Review

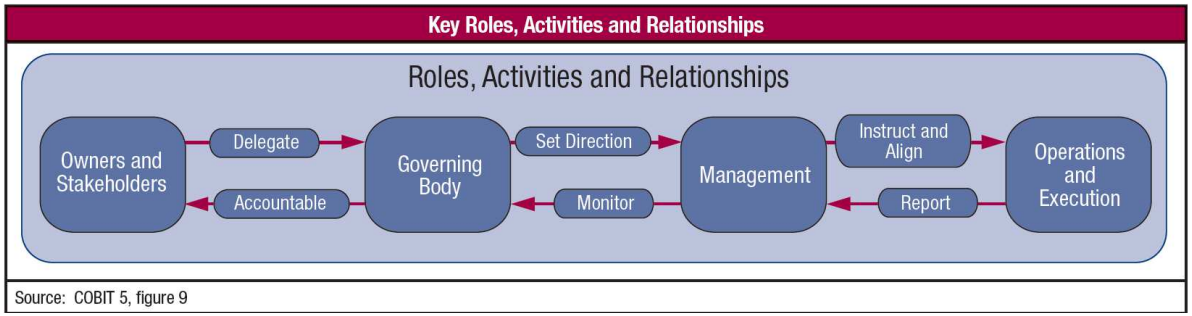
John Kenneth Barchie
CISM, CRISC, CISSP

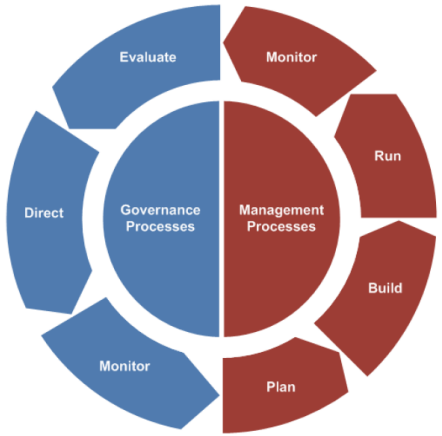
www.barchieconsulting.com

COBIT 5 Tools of the Framework

- Governance
- Enablers
- Principles
- BMIS
- Replaces/Augments COSO for SOX
- PCA replaces CMM
  - N,P,L,F

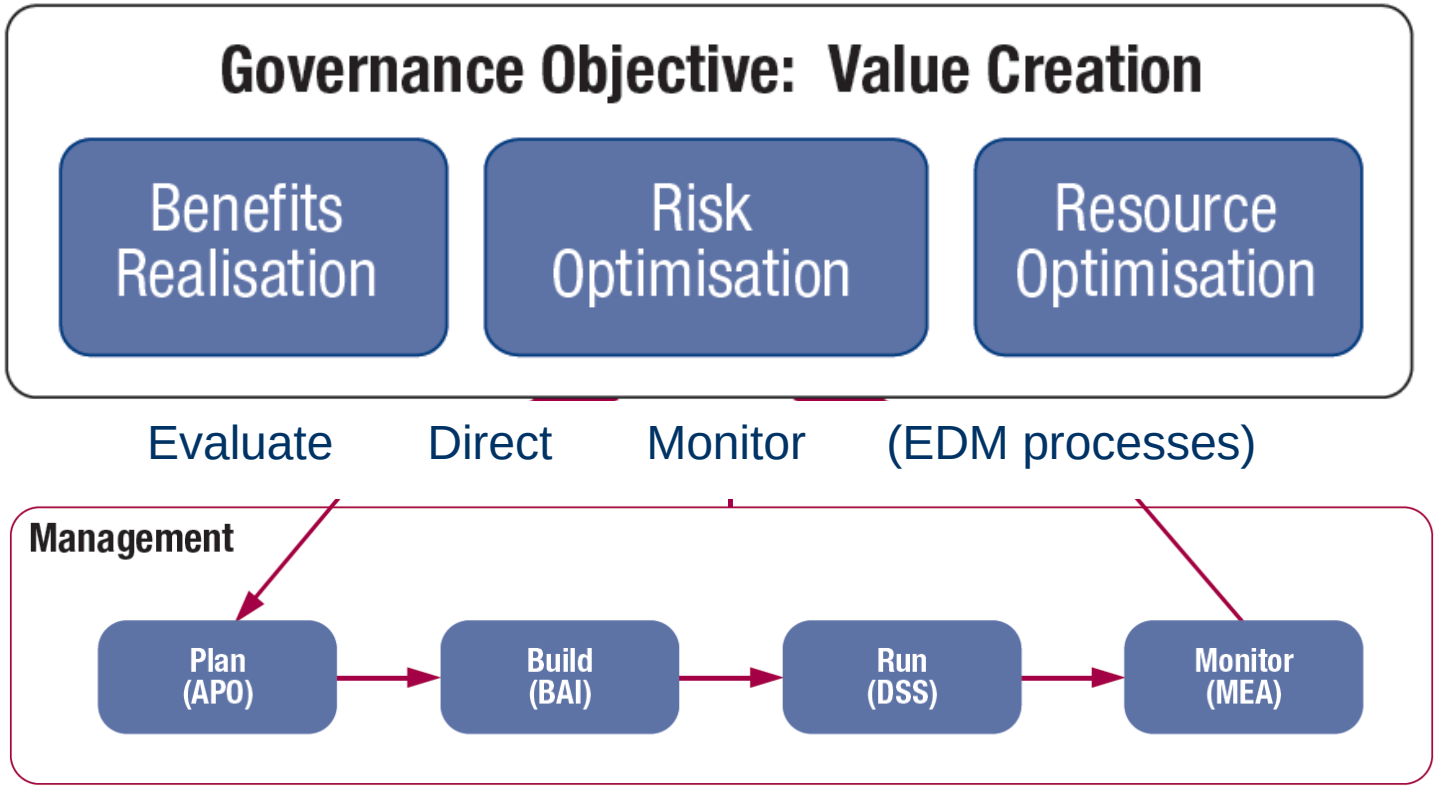
COBIT 5 Governance



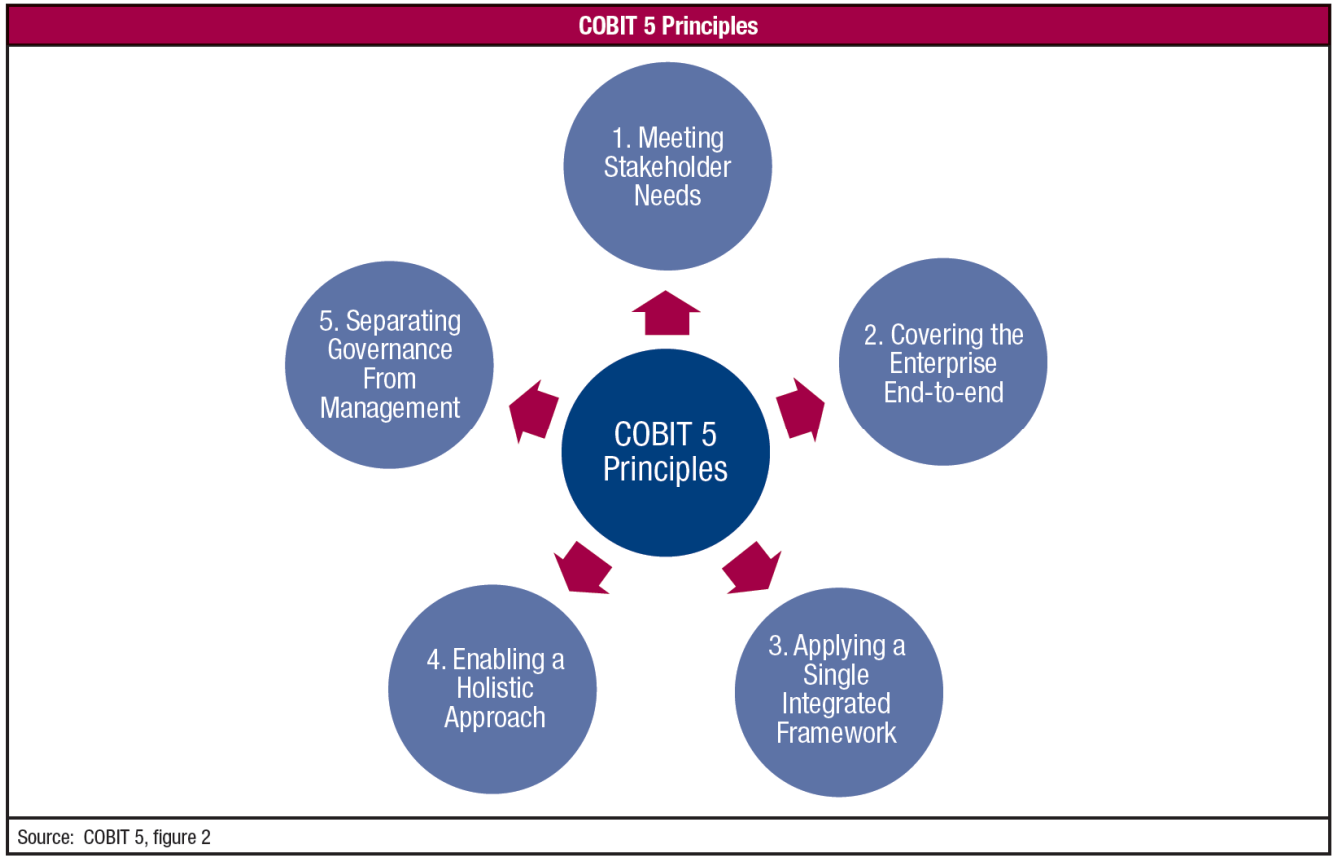


← Love this graphic

COBIT 5 Difference between Governance and Management

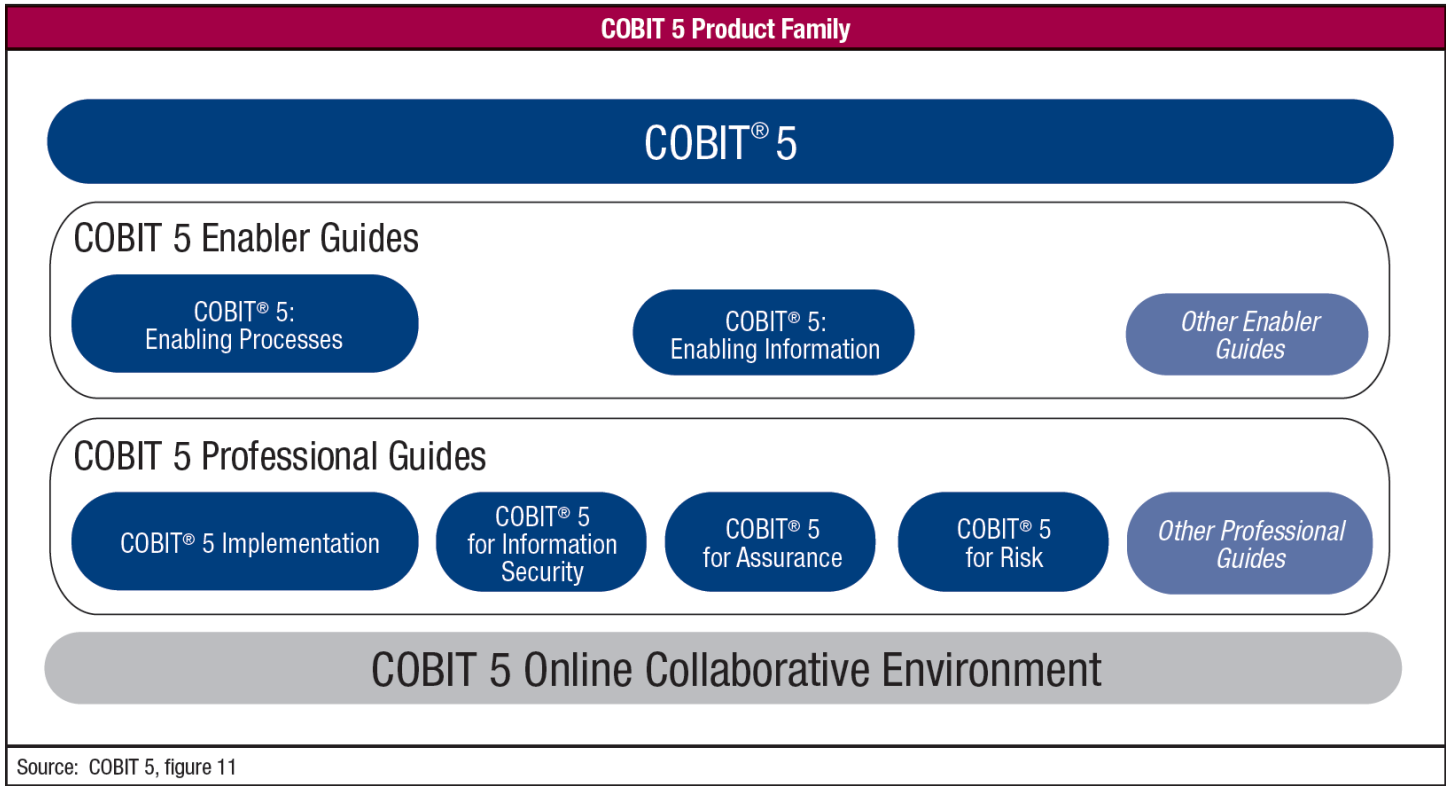


COBIT 5 Principles



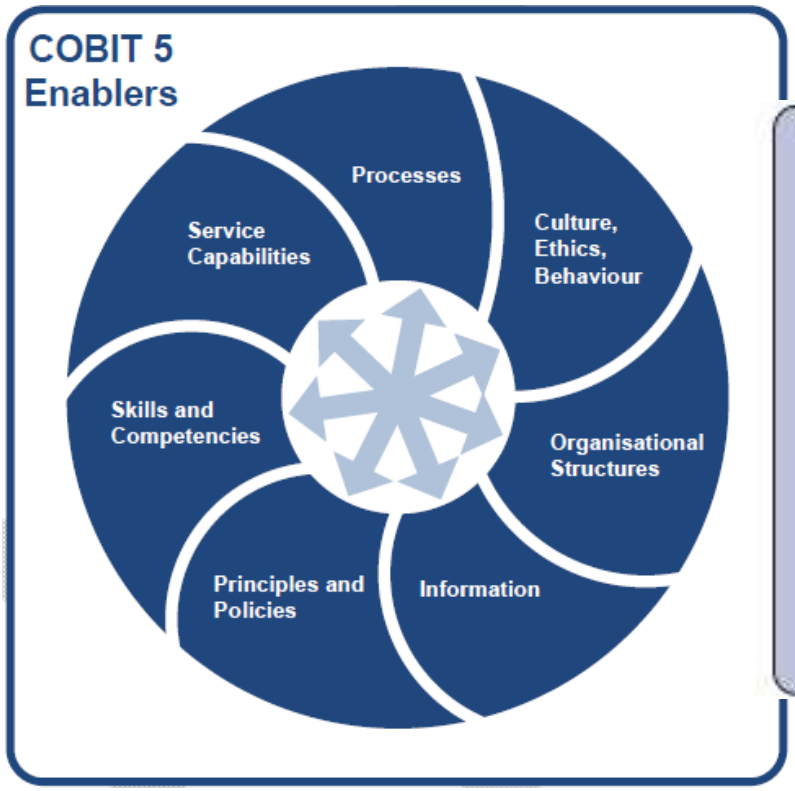
Source: COBIT 5, figure 2

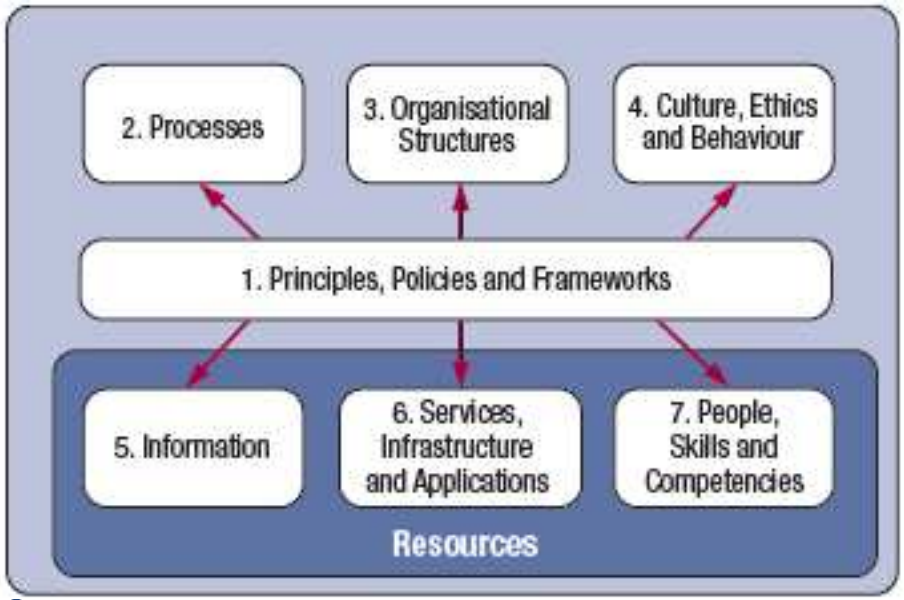
COBIT 5 Product Family



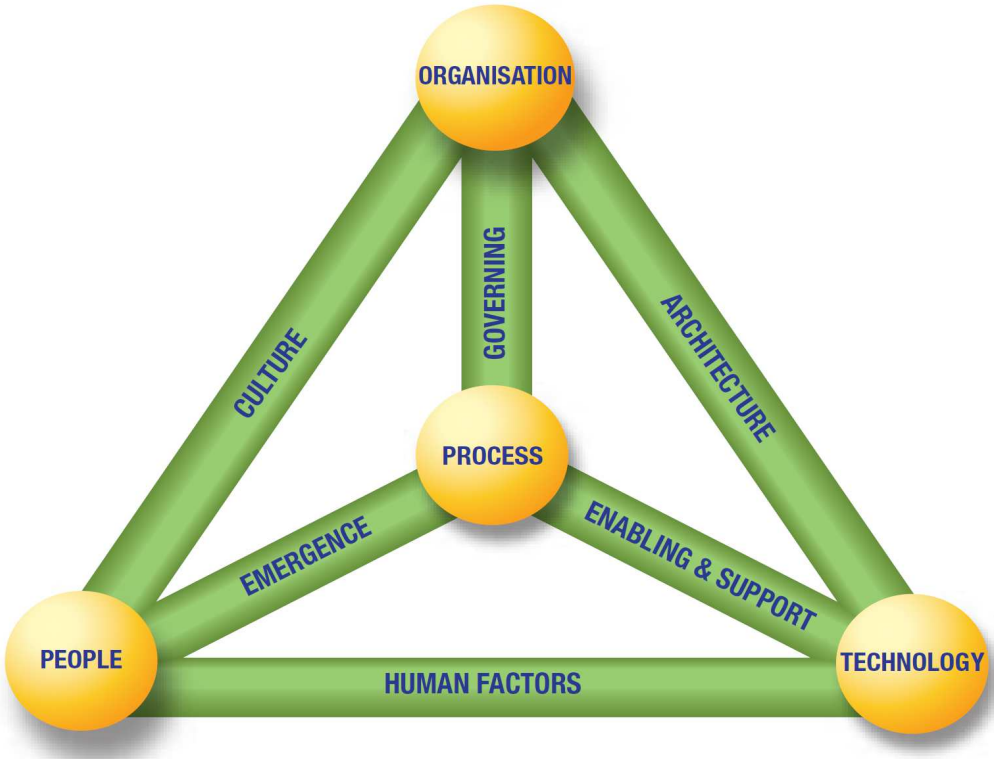
Source: COBIT 5, figure 11

COBIT 5 Enablers



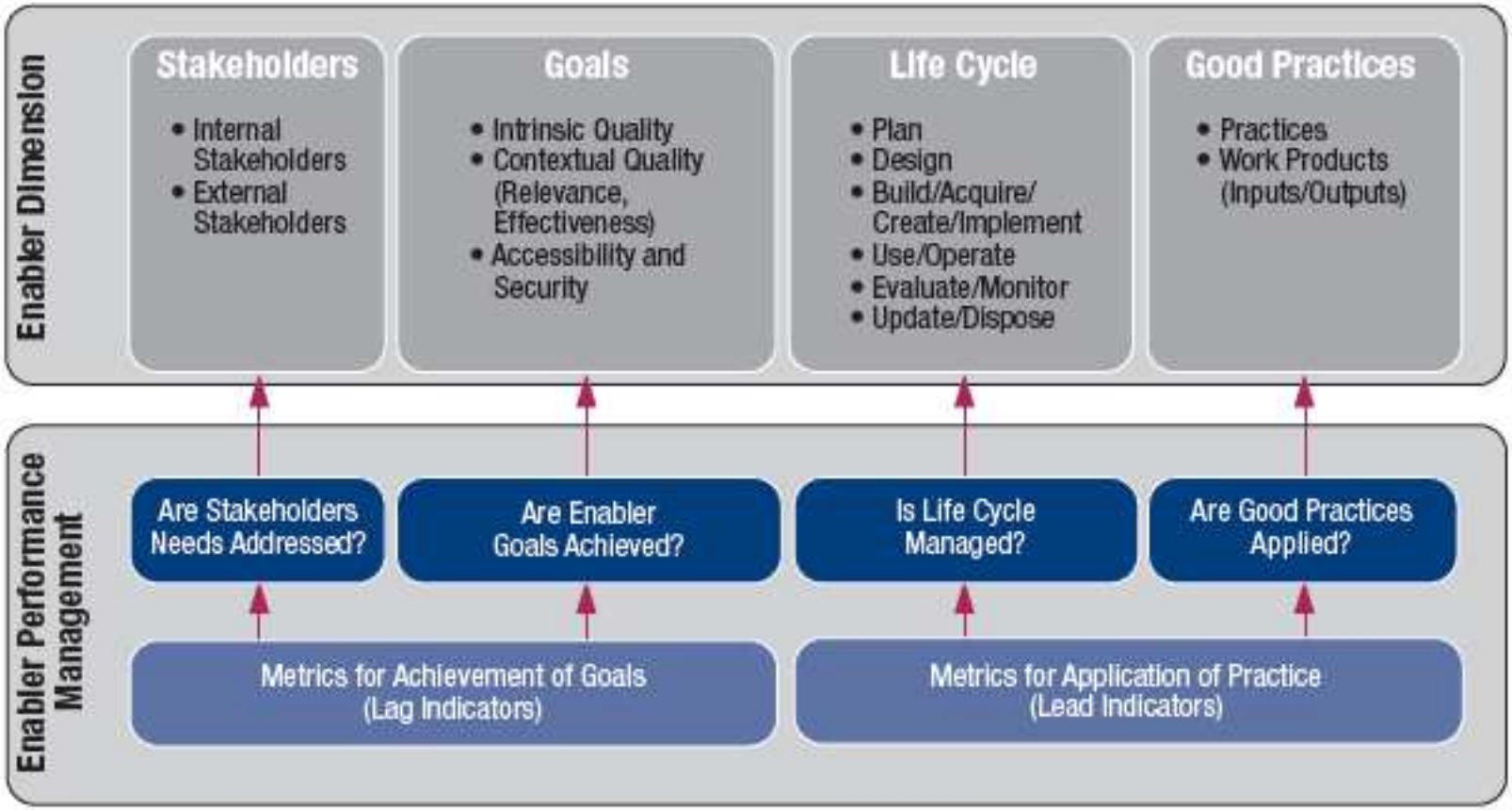


COBIT 5 and BMIS

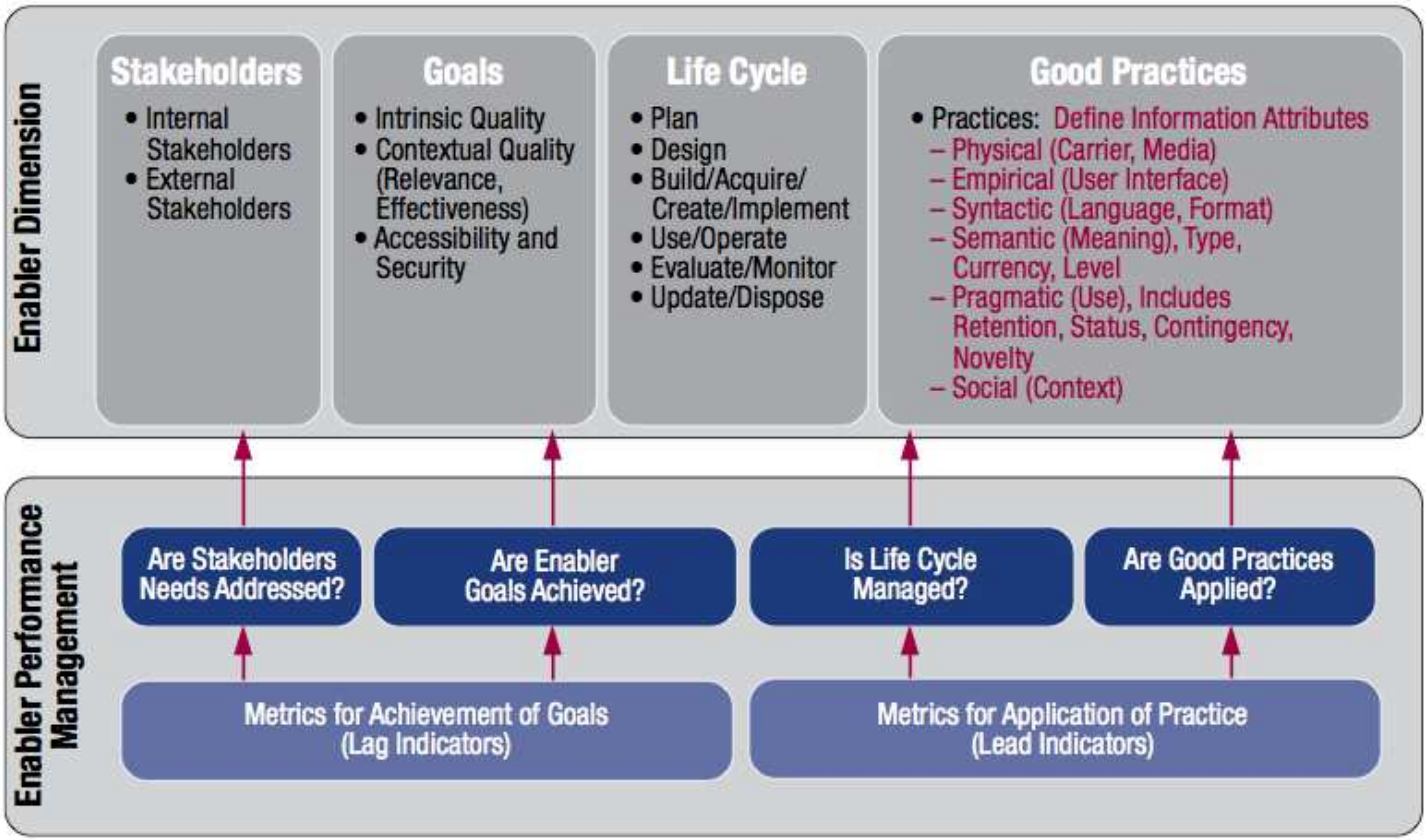


COBIT 5 Goals Cascade

COBIT 5 Generic Enabler Model



COBIT 5 Information Enabler Model



COBIT 5 Goodbye CMM

Process Capability Attribute

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

Process Optimization and innovation
Process Control and Management

Process Deployment
Process Definition

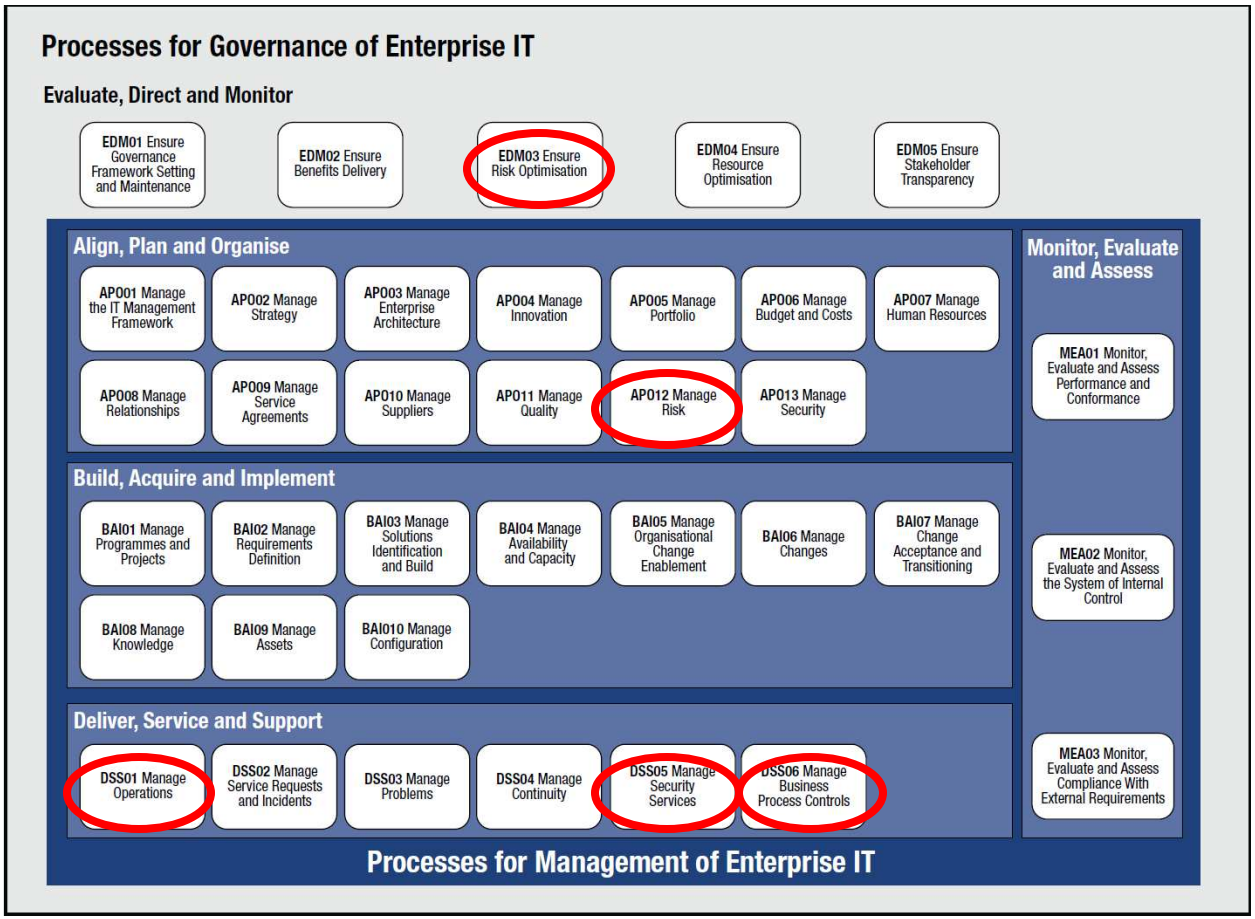
Work Product Management
Performance Management

Process Performance –
Be Careful with Ad Hoc
-jkb

COBIT 5 Other tools not used in this report

- RACI charts
- Mapping of Goals to Processes
- Mapping of Stakeholder needs
- Val IT
- Direction Diagram
- Metrics

Actually used in supplement



Use of the Metrics

EDM03 Ensure Risk Optimisation	Area: Governance Domain: Evaluate, Direct and Monitor
Process Description Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.	
Process Purpose Statement Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update or risk profile
06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines
15 IT compliance with internal policies	• Number of incidents related to non-compliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices • Frequency of policies review and update
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Risk thresholds are defined and communicated and key IT-related risk is known.	• Level of alignment between IT risk and enterprise risk • Number of potential IT risks identified and managed • Refreshment rate of risk factor evaluation
2. The enterprise is managing critical IT-related enterprise risk effectively and efficiently.	• Percent of enterprise projects that consider IT risk • Percent of IT risk action plans executed on time • Percent of critical risk that has been effectively mitigated
3. IT-related enterprise risk does not exceed risk appetite and the impact of IT risk to enterprise value is identified and managed.	• Level of unexpected enterprise impact • Percent of IT risk that exceeds enterprise risk tolerance

RACI Chart

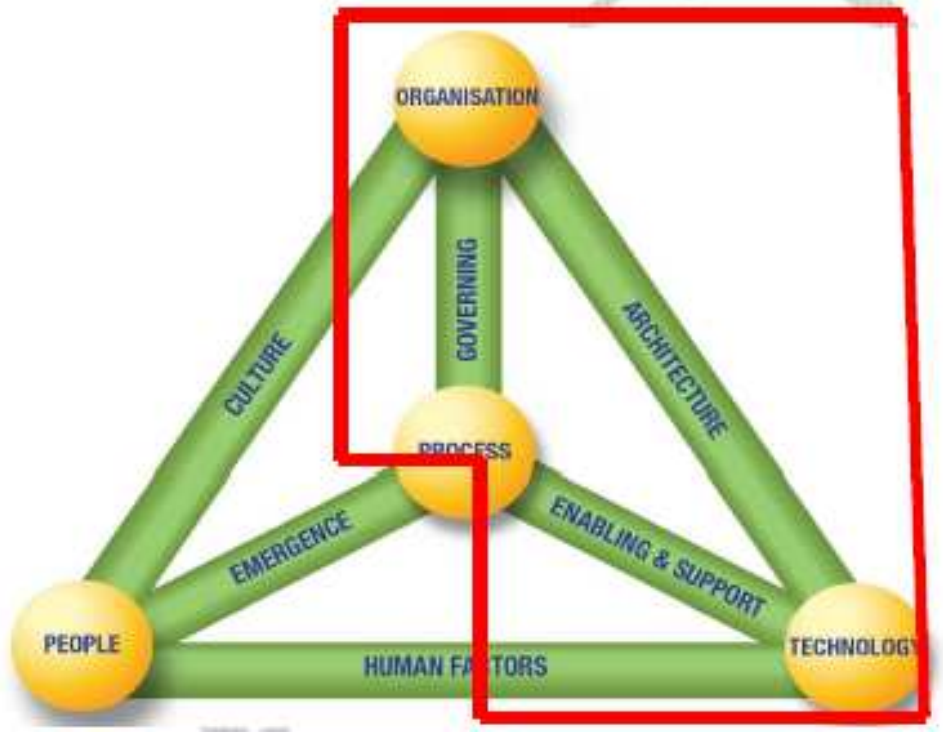
AP012 RACI Chart																											
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP012.01 Collect data.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
AP012.02 Analyse risk.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
AP012.03 Maintain a risk profile.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
AP012.04 Articulate risk.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
AP012.05 Define a risk management action portfolio.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
AP012.06 Respond to risk.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Set up a table to show activities

COBIT 5 Reference	PCI DSS Reference	COBIT 5 recommended activity
EDM01.01	12.1	Determine the significance of IT and its role with respect to the business.
EDM01.01	12.1.1	Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise IT.
EDM03.01	12.1.2	Proactively evaluate IT risk factors in advance of pending strategic enterprise decisions and ensure that risk-aware enterprise decisions are made.
EDM03.01	12.1.2	Determine that IT use is subject to appropriate risk assessment and evaluation, as described in relevant international and national standards
EDM03.02	12.1.2	Direct the integration of the IT risk strategy and operations with the enterprise strategic risk decisions and operations.

COBIT 5 Report Tools Used Setting the Scope

FIG 1: Items encircled in red were covered in the scope of this review



COBIT 5 Providing the Process Capabilities Assessment

Service Provider Initiative Executive Dashboard	Business Segregation	PCI Compliance	Valid Architecture
Due Diligence			
Implementation Costs			
Disaster Recovery			

Red indicates incomplete status, Yellow indicates performed status and Green Indicates managed status.

COBIT 5 Documenting the Enablers

- Network Diagrams
  - Iterative descriptions
- Risk Assessments
  - Provided Training

COBIT 5 Stakeholder Needs

- Understand the risk
- Understand the cost of doing business
- Direct and Monitor Management

COBIT 5 Advantages Page 17

- The starting point of governance and management activities are 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 an end - to - end view on all IT - related matters
- Provides a systemic view

• Creates a common language between IT and business for the enterprise governance and management of IT

Thank you for your time, Questions?

- John Kenneth Barchie, CISM, CRISC etc…
  - Sr. Security Consultant for IPI International
    - jbarchie@infoplusintl.com
  - President of Barchie Consulting
    - jbarchie@barchieconsulting.com
    - 408-425-3899
    - www.barchieconsulting.com
  - President of (ISC)2 Silicon Valley Chapter
    - president@isc2-siliconvalley-chapter.org
  - God Bless!