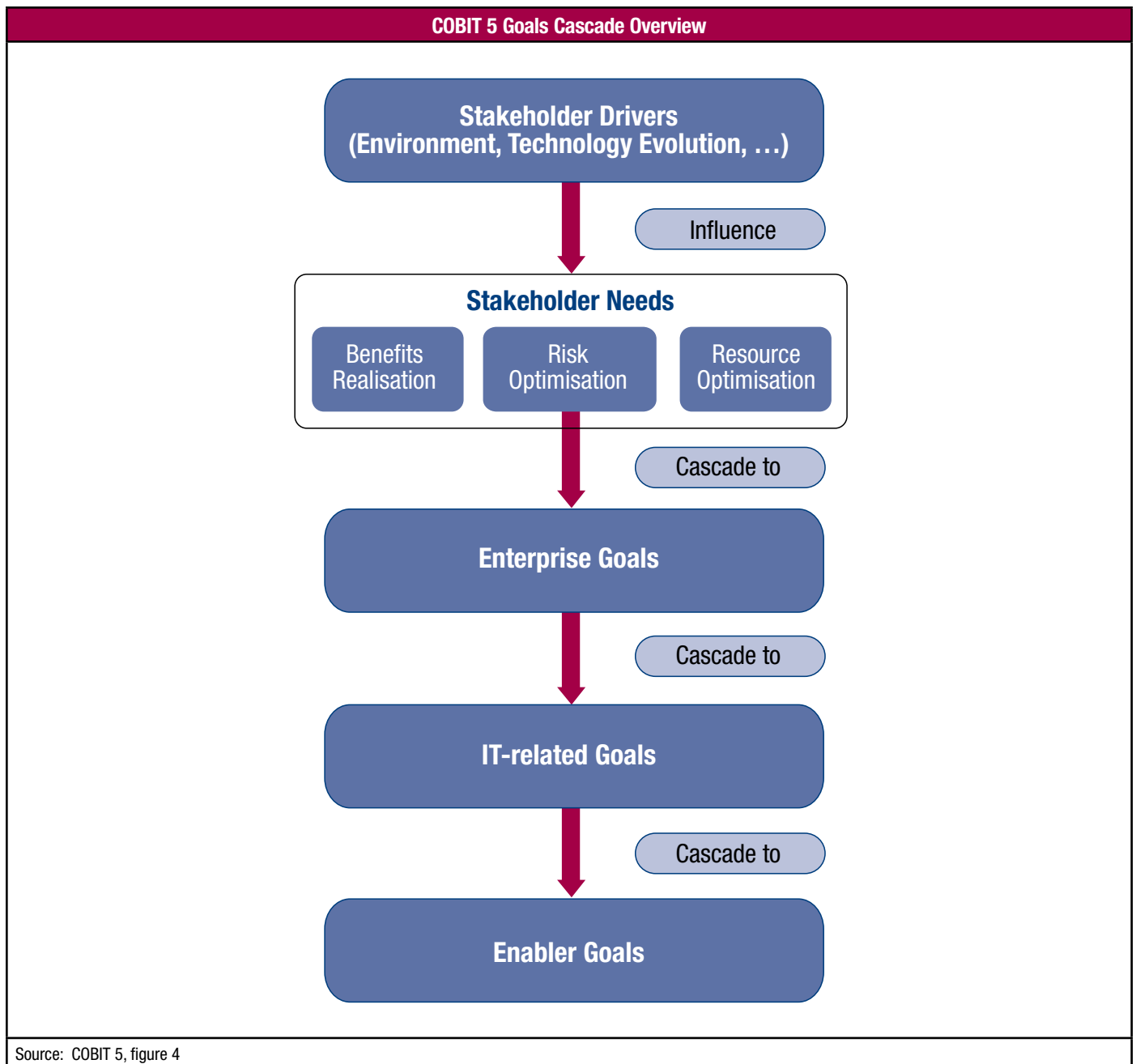


3701 Algonquin Road, Suite 1010 • Rolling Meadows, IL 60008 USA
 Phone: +1.847.253.1545 • Fax: +1.847.253.1443 • Email: info@isaca.org
 Web site: www.isaca.org

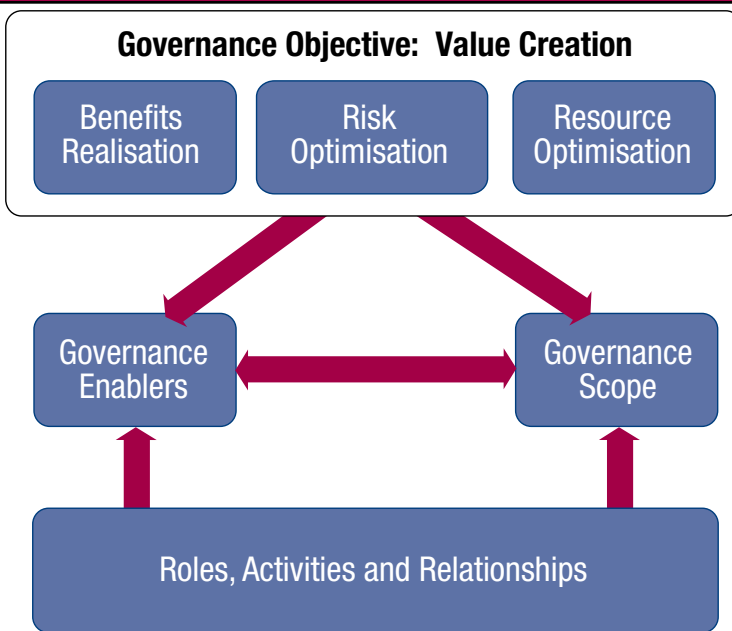


Selected Guidance From the COBIT 5 Family

These charts and figures are elements of COBIT 5 and its supporting guides. This excerpt is available as a complimentary PDF (www.isaca.org/cobit) and for purchase in hard copy (www.isaca.org/bookstore). It provides an overview of the COBIT 5 guidance, its five principles and seven enablers. We encourage you to share this document with your enterprise leaders, team members, clients and/or consultants.

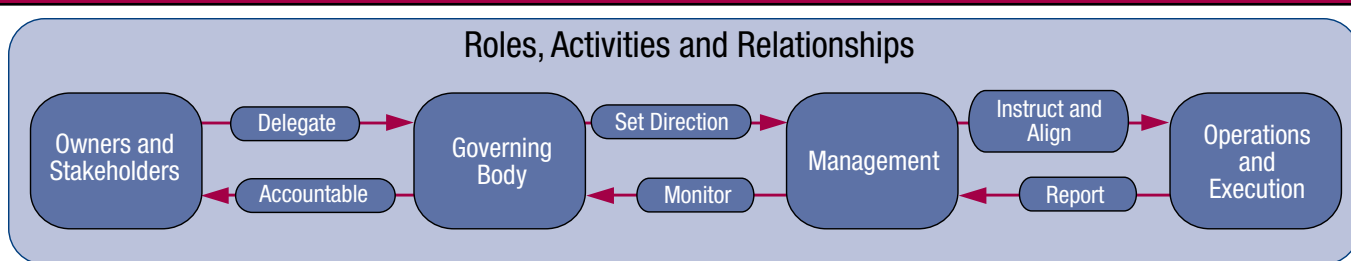
COBIT enables enterprises to maximize the value and minimize the risk related to information, which has become the currency of the 21st century. COBIT 5 is a comprehensive framework of globally accepted principles, practices, analytical tools and models that can help any enterprise effectively address critical business issues related to the governance and management of information and technology. Additional information is available at www.isaca.org/cobit.

Governance and Management in COBIT 5



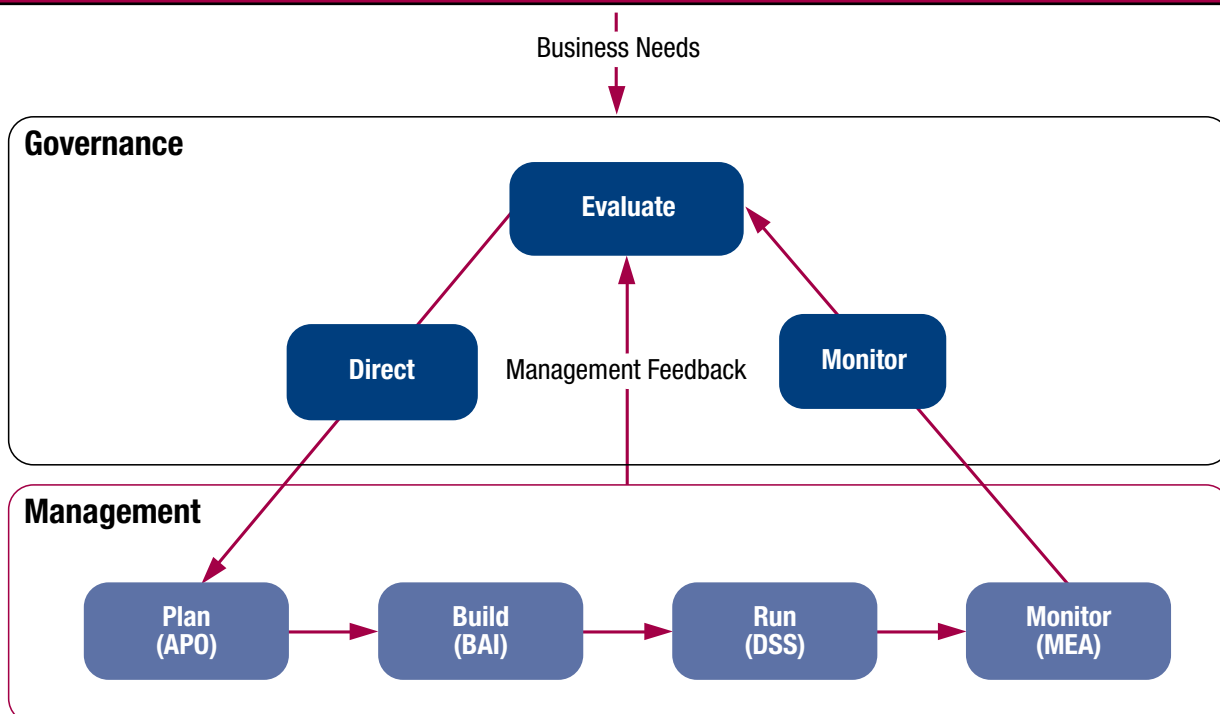
Source: COBIT 5, figure 8

Key Roles, Activities and Relationships



Source: COBIT 5, figure 9

COBIT 5 Governance and Management Key Areas



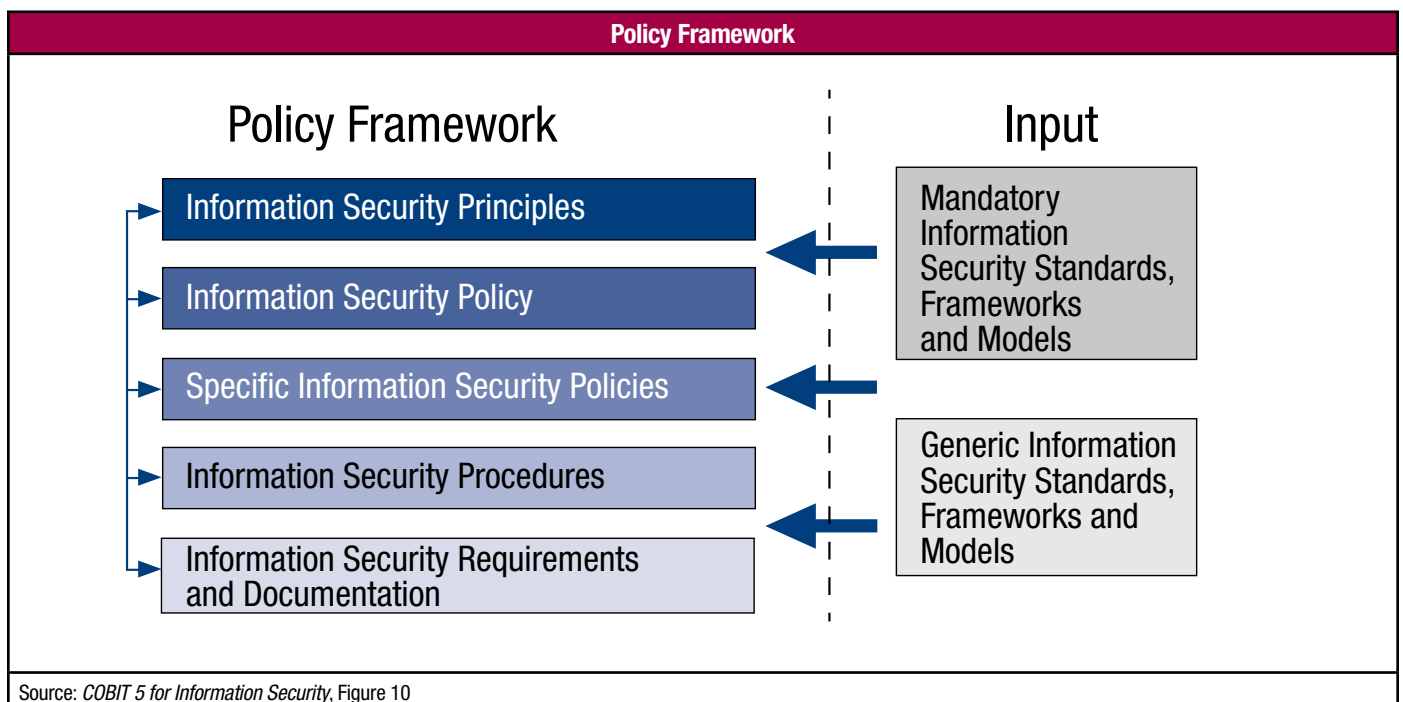
Source: COBIT 5, figure 15

Information Security Skills/Competencies
Skills/Competencies
Information security governance
Information security strategy formulation
Information risk management
Information security architecture development
Information security operations
Information assessment and testing and compliance
Source: COBIT 5 for Information Security, Figure 20

Example Stakeholders for Information Security-related Information (Small/Medium Enterprise)										
Stakeholder	Information Type									
	Information Security Strategy	Information Security Budget	Information Security Plan	Policies	Information Security Requirements	Awareness Material	Information Security Review Reports	Information Security Service Catalogue	Information Risk Profile	Information Security Dashboard
Internal: Enterprise										
Board	U			I		U	I		A	
Chief executive officer (CEO)	U			A		U	I		U	
Chief financial officer (CFO)		A		U		U			U	
Chief information security officer (CISO)	O	U	O	O	A	A	A	A	U	U
Information security steering committee (ISSC)	A	O	A	U	U	I	U	I	U	U
Business process owner				U	O	U		U	U	
Head of human resources (HR)				U		U				
Internal: IT										
Chief information officer (CIO)/IT manager	U	O	U	U	U	U	I		U	U
Information security manager (ISM)	U	U	U	O	U	O	O	O	O	O
External										
Investors						I				
Insurers						I	I		I	
Regulators		I				I	I			
Business Partners						I	I			
Vendors/Suppliers						I				
External Auditors		I				I	I		I	I
<p>An indication of the nature of the relationship of the stakeholder for each information type:</p> <p>A—Approver</p> <p>O—Originator</p> <p>I—Informed of information type</p> <p>U—User of information type</p>										
Source: COBIT 5 for Information Security, Figure 17										

Advantages and Disadvantages of Potential Paths for Information Security Reporting		
Role	Advantages	Disadvantages
Chief executive officer (CEO)	Information risk is elevated to the highest level in the enterprise.	Information risk needs to be presented in a format that is understandable to the CEO. Given the multitude of responsibilities of the CEO, information risk might be monitored and managed at too high a level of abstraction or might not be fully understood in its relevant details.
Chief information officer (CIO)	Information security issues and solutions can be aligned with all IT initiatives.	Information risk may not be addressed due to other IT initiatives and deadlines taking precedence over information security. There is a potential conflict of interest. The work performed by information security professionals may be IT-focussed and not information security-focussed. In other words, there may be an insufficient business focus.
Chief financial officer (CFO)	Information security issues can be addressed from a financial business impact point of view.	Information risk may not be addressed due to financial initiatives and deadlines taking precedence over information security. There is a potential conflict of interest.
Chief risk officer (CRO)	Information risk is elevated to a position that can also look at risk from strategic, financial, operational, reputational and compliance perspectives.	This role does not exist in most enterprises. It is most often found in financial service organisations. In enterprises in which a CRO is not present, organisational risk decisions may be decided by the CEO or board of directors.
Chief technology officer (CTO)	Information security can be partnered and included in future technology road maps.	Information risk may not be addressed due to technology directions taking precedence over information security.
Chief operating officer (COO)	Information security issues and solutions can be addressed from the standpoint of impact to the business' operations.	Information risk may not be addressed due to operational initiatives and deadlines taking precedence over information security.
Board of directors (indirect report)	Information risk is elevated to the highest level in the enterprise.	Information risk needs to be presented in a format that is understandable to board members, and hence may become too high-level to be relevant.

Source: COBIT 5 for Information Security, Figure 14



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- AP001 Manage the IT Management Framework
- AP002 Manage Strategy
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Portfolio
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP010 Manage Suppliers
- AP011 Manage Quality
- AP012 Manage Risk
- AP013 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

