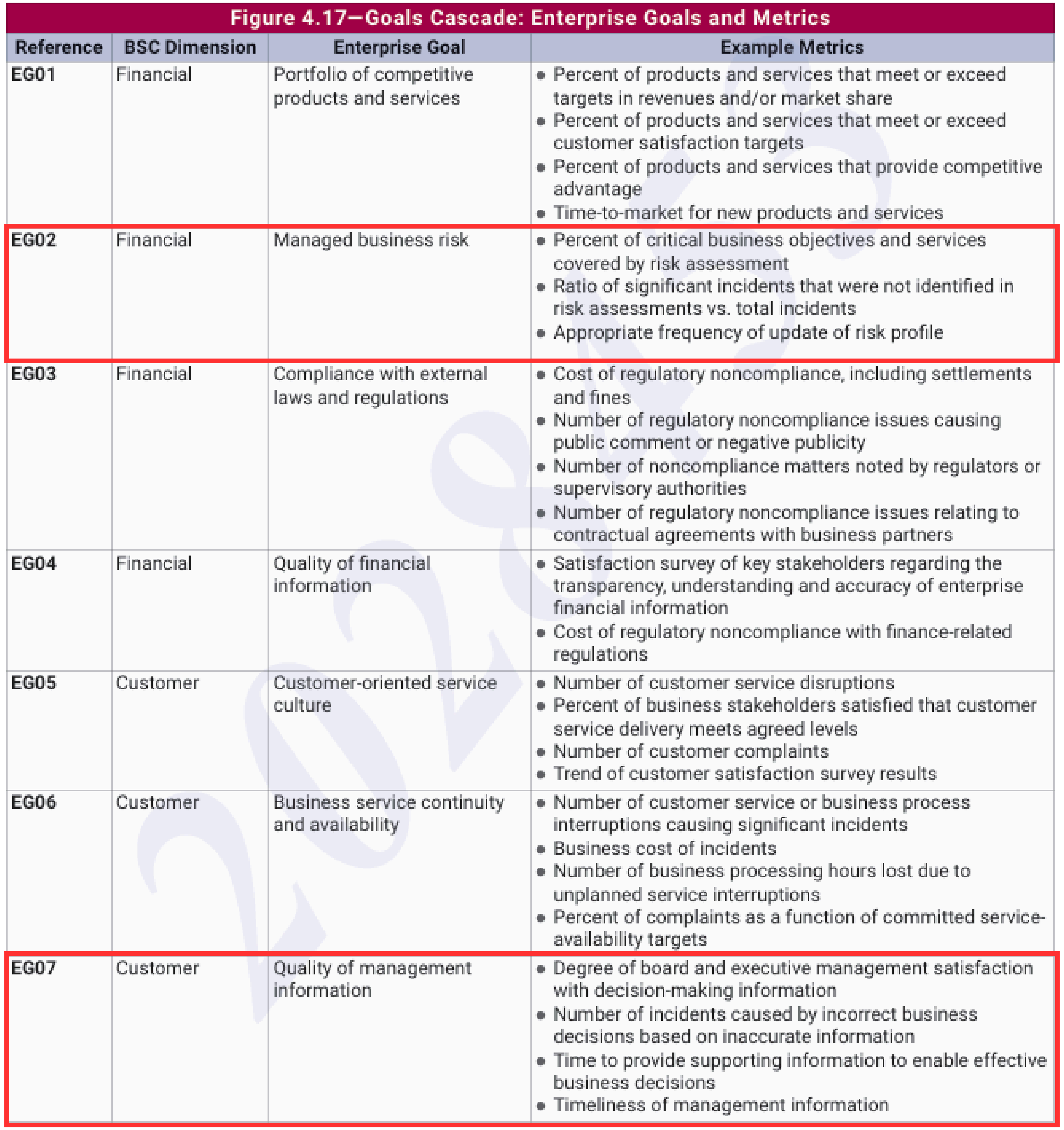
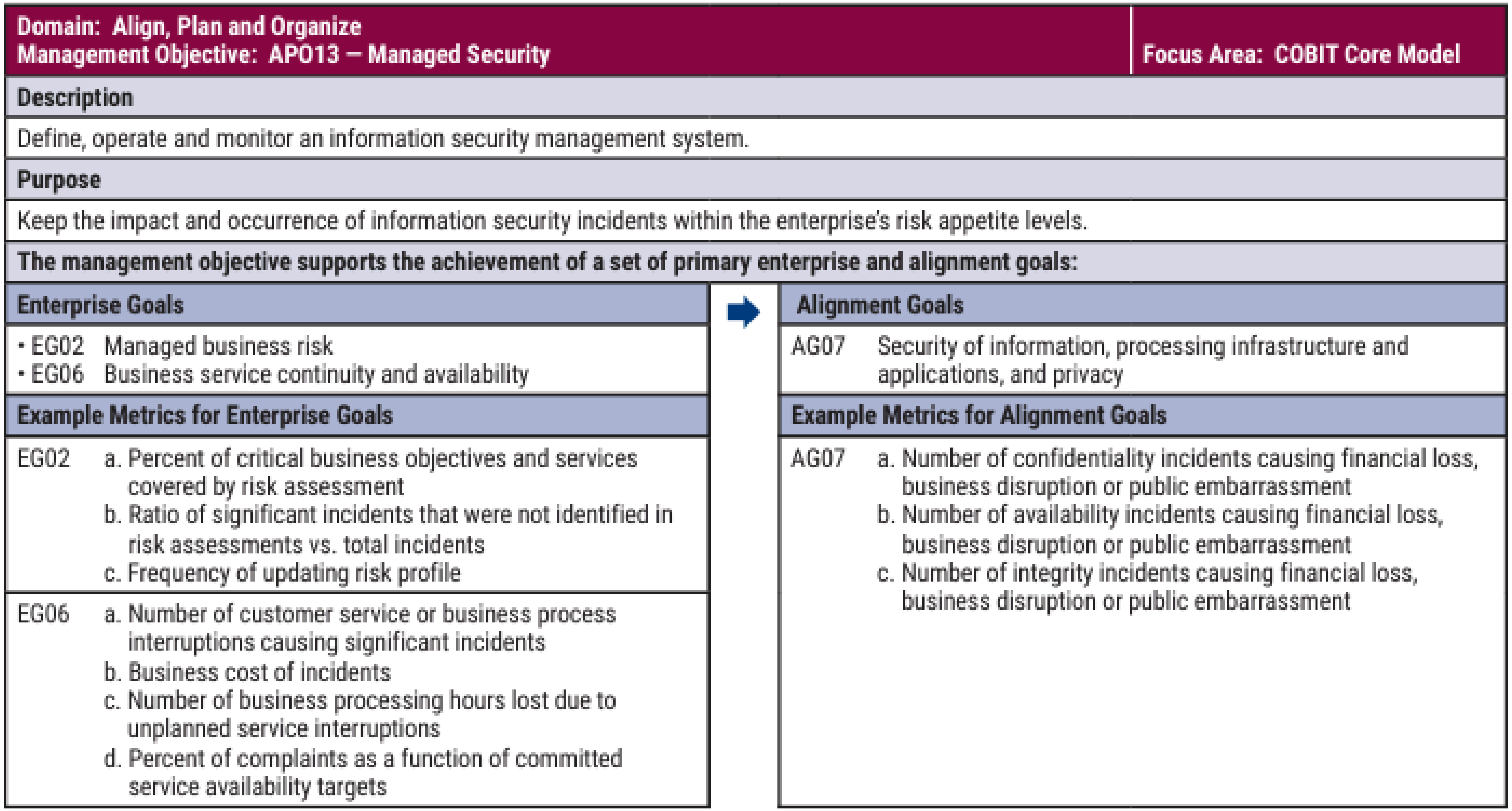
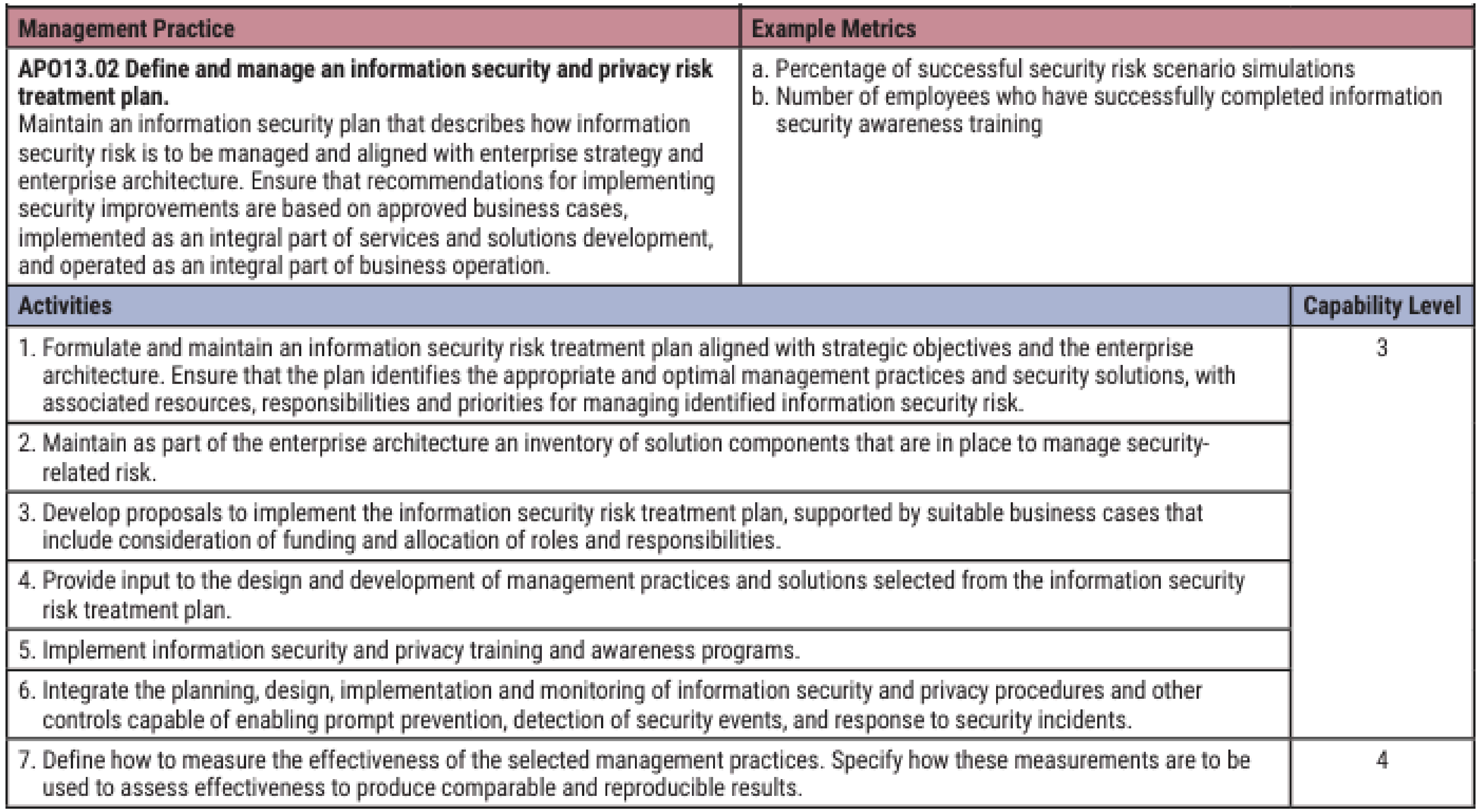


Figure 4.17—Goals Cascade: Enterprise Goals and Metrics

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG01	Financial	Portfolio of competitive products and services	• Percent of products and services that meet or exceed targets in revenues and/or market share • Percent of products and services that meet or exceed customer satisfaction targets • Percent of products and services that provide competitive advantage • Time-to-market for new products and services
EG02	Financial	Managed business risk	• Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identified in risk assessments vs. total incidents • Appropriate frequency of update of risk profile
EG03	Financial	Compliance with external laws and regulations	• Cost of regulatory noncompliance, including settlements and fines • Number of regulatory noncompliance issues causing public comment or negative publicity • Number of noncompliance matters noted by regulators or supervisory authorities • Number of regulatory noncompliance issues relating to contractual agreements with business partners
EG04	Financial	Quality of financial information	• Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information • Cost of regulatory noncompliance with finance-related regulations
EG05	Customer	Customer-oriented service culture	• Number of customer service disruptions • Percent of business stakeholders satisfied that customer service delivery meets agreed levels • Number of customer complaints • Trend of customer satisfaction survey results
EG06	Customer	Business service continuity and availability	• Number of customer service or business process interruptions causing significant incidents • Business cost of incidents • Number of business processing hours lost due to unplanned service interruptions • Percent of complaints as a function of committed service-availability targets
EG07	Customer	Quality of management information	• Degree of board and executive management satisfaction with decision-making information • Number of incidents caused by incorrect business decisions based on inaccurate information • Time to provide supporting information to enable effective business decisions • Timeliness of management information

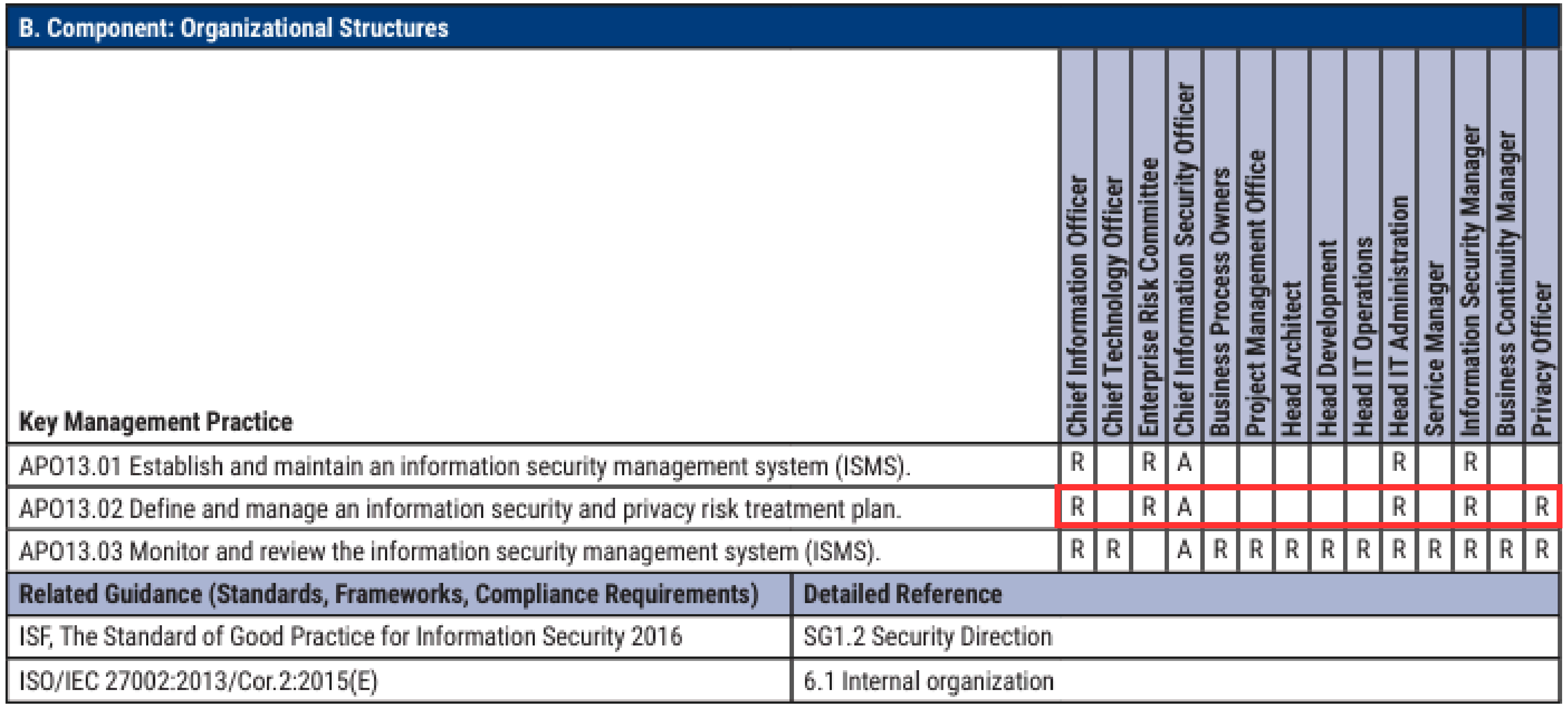


Domain: Align, Plan and Organize Management Objective: APO13 — Managed Security	Focus Area: COBIT Core Model
Description	
Define, operate and monitor an information security management system.	
Purpose	
Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.	
The management objective supports the achievement of a set of primary enterprise and alignment goals:	
Enterprise Goals	**Alignment Goals**
• EG02 Managed business risk • EG06 Business service continuity and availability	AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets	



Management Practice	Example Metrics
APO13.02 Define and manage an information security and privacy risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases, implemented as an integral part of services and solutions development, and operated as an integral part of business operation.	a. Percentage of successful security risk scenario simulations b. Number of employees who have successfully completed information security awareness training

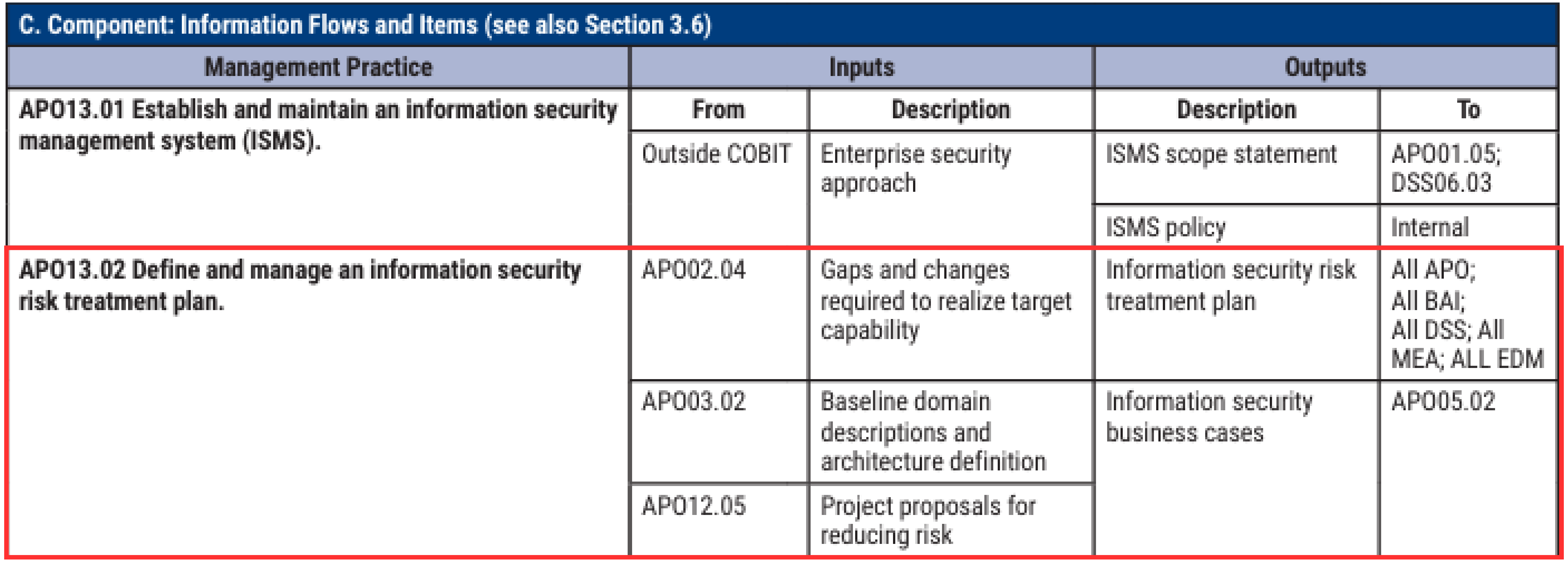
Activities	Capability Level
1. Formulate and maintain an information security risk treatment plan aligned with strategic objectives and the enterprise architecture. Ensure that the plan identifies the appropriate and optimal management practices and security solutions, with associated resources, responsibilities and priorities for managing identified information security risk.	3
2. Maintain as part of the enterprise architecture an inventory of solution components that are in place to manage security-related risk.	
3. Develop proposals to implement the information security risk treatment plan, supported by suitable business cases that include consideration of funding and allocation of roles and responsibilities.	
4. Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan.	
5. Implement information security and privacy training and awareness programs.	
6. Integrate the planning, design, implementation and monitoring of information security and privacy procedures and other controls capable of enabling prompt prevention, detection of security events, and response to security incidents.	
7. Define how to measure the effectiveness of the selected management practices. Specify how these measurements are to be used to assess effectiveness to produce comparable and reproducible results.	4



B. Component: Organizational Structures

Key Management Practice	Chief Information Officer	Chief Technology Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO13.01 Establish and maintain an information security management system (ISMS).	R		R	A						R		R		
APO13.02 Define and manage an information security and privacy risk treatment plan.	R		R	A						R		R		R
APO13.03 Monitor and review the information security management system (ISMS).	R	R		A	R	R	R	R	R	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SG1.2 Security Direction
ISO/IEC 27002:2013/Cor.2:2015(E)	6.1 Internal organization

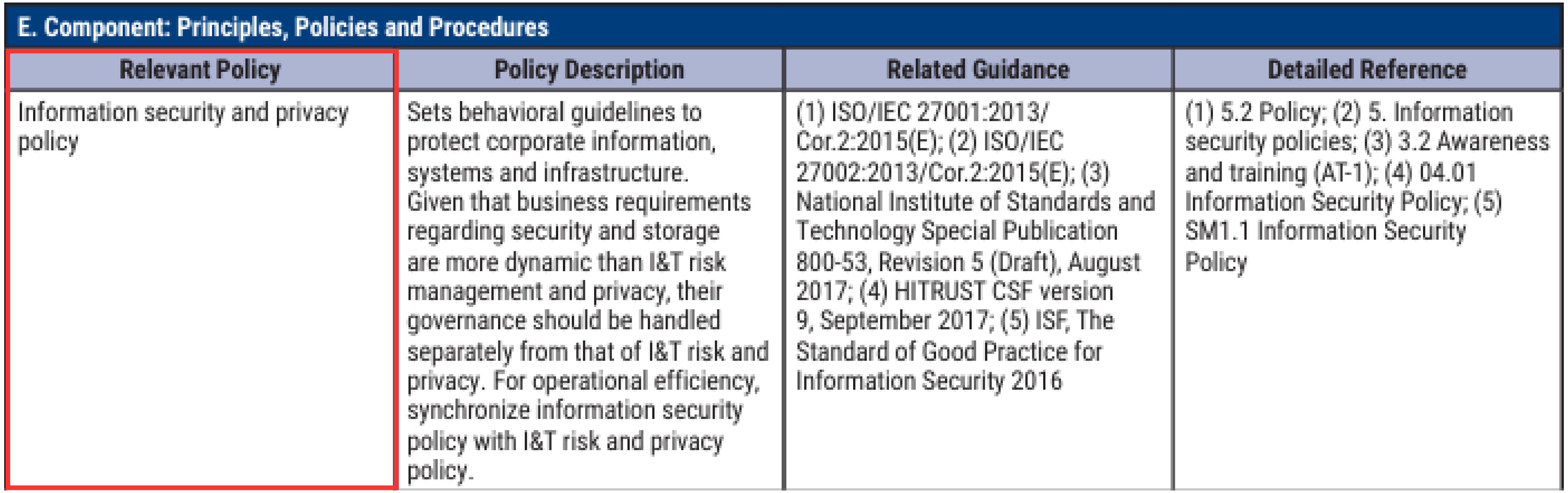


C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO13.01 Establish and maintain an information security management system (ISMS).	Outside COBIT	Enterprise security approach	ISMS scope statement	APO01.05; DSS06.03
			ISMS policy	Internal

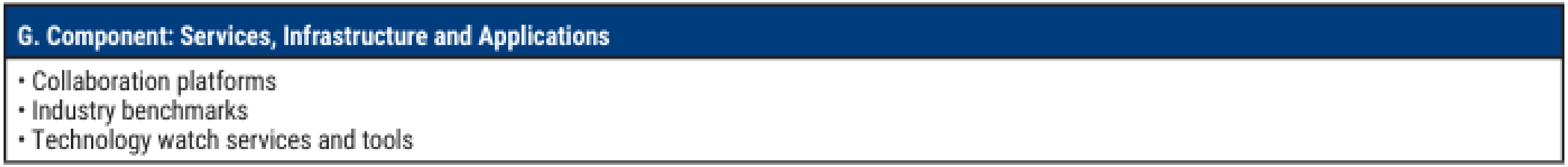
APO13.02 Define and manage an information security risk treatment plan.	APO02.04	Gaps and changes required to realize target capability	Information security risk treatment plan	All APO;
				All BAI;
				All DSS; All MEA; ALL EDM

	APO03.02	Baseline domain descriptions and architecture definition	Information security business cases	APO05.02
	APO12.05	Project proposals for reducing risk		



E. Component: Principles, Policies and Procedures

Relevant Policy	Policy Description	Related Guidance	Detailed Reference
Information security and privacy policy	Sets behavioral guidelines to protect corporate information, systems and infrastructure. Given that business requirements regarding security and storage are more dynamic than I&T risk management and privacy, their governance should be handled separately from that of I&T risk and privacy. For operational efficiency, synchronize information security policy with I&T risk and privacy policy.	(1) ISO/IEC 27001:2013/ Cor.2:2015(E); (2) ISO/IEC 27002:2013/Cor.2:2015(E); (3) National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017; (4) HITRUST CSF version 9, September 2017; (5) ISF, The Standard of Good Practice for Information Security 2016	(1) 5.2 Policy; (2) 5. Information security policies; (3) 3.2 Awareness and training (AT-1); (4) 04.01 Information Security Policy; (5) SM1.1 Information Security Policy



G. Component: Services, Infrastructure and Applications
• Collaboration platforms • Industry benchmarks • Technology watch services and tools