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	

A. Component: Process	
Management Practice	**Example Metrics**
APO13.01 Establish and maintain an information security management system (ISMS). Establish and maintain an information security management system (ISMS) that provides a standard, formal and continuous approach to information security management, enabling secure technology and business processes that are aligned with business requirements.	a. Level of stakeholder satisfaction with the security plan throughout the enterprise

Activities	Capability Level
1. Define the scope and boundaries of the information security management system (ISMS) in terms of the characteristics of the enterprise, the organization, its location, assets and technology. Include details of, and justification for, any exclusions from the scope.	2
2. Define an ISMS in accordance with enterprise policy and the context in which the enterprise operates.	
3. Align the ISMS with the overall enterprise approach to the management of security.	
4. Obtain management authorization to implement and operate or change the ISMS.	
5. Prepare and maintain a statement of applicability that describes the scope of the ISMS.	
6. Define and communicate information security management roles and responsibilities.	
7. Communicate the ISMS approach.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	0.01 Information Security Management program
ISO/IEC 20000-1:2011(E)	6.6 Information security management
ITIL V3, 2011	Service Design, 4.7 Information Security Management
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 1); 3.4 Implementation (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-2)
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
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
APO13.03 Monitor and review the information security management system (ISMS). Maintain and regularly communicate the need for, and benefits of, continuous improvement in information security. Collect and analyze data about the information security management system (ISMS), and improve its effectiveness. Correct nonconformities to prevent recurrence.	a. Frequency of scheduled security reviews b. Number of findings in regularly scheduled security reviews c. Level of stakeholder satisfaction with the security plan d. Number of security-related incidents caused by failure to adhere to the security plan

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Undertake regular reviews of the effectiveness of the ISMS. Include meeting ISMS policy and objectives and reviewing security and privacy practices.	4
2. Conduct ISMS audits at planned intervals.	
3. Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified.	
4. Record actions and events that could have an impact on the effectiveness or performance of the ISMS.	
5. Provide input to the maintenance of the security plans to take into account the findings of monitoring and reviewing activities.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 3)

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		

C. Component: Information Flows and Items (see also Section 3.6) (cont.)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO13.03 Monitor and review the information security management system (ISMS).	DSS02.02	Classified and prioritized incidents and service requests	Recommendations for improving the information security management system (ISMS)	Internal
			Information security management system (ISMS) audit reports	MEA02.01
Related Guidance (Standards, Frameworks, Compliance Requirements)		Detailed Reference		
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017		3.3 Selection (Tasks 1, 3): Inputs and Outputs; 3.4 Implementation (Task 1): Inputs and Outputs		

D. Component: People, Skills and Competencies		
Skill	Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Information security	Skills Framework for the Information Age V6, 2015	SCTY
Information security strategy development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.1. Information Security Strategy Development

E. Component: 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

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	Related Guidance	Detailed Reference
Establish a culture of security and privacy awareness that positively influences desirable behavior and actual implementation of security and privacy policy in daily practice. Provide sufficient security and privacy guidance, indicate security and privacy champions (including C-level executives, leaders in HR, and security and/or privacy professionals) and proactively support and communicate security and privacy programs, innovations and challenges.	(1) ISO/IEC 27001:2013/ Cor.2:2015(E); (2) Creating a Culture of Security, ISACA, 2011	1) 7.3 Awareness; (2) Framework to achieve an intentional security aware culture (all chapters)

G. Component: Services, Infrastructure and Applications
• Configuration management tools • Security and privacy awareness services • Third-party security assessment services