APO13 Manage Security	Area: Management Domain: Align, Plan and Organise
Process Description Define, operate and monitor a system for information security management.	
Process Purpose Statement Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
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 of 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
14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. A system is in place that considers and effectively addresses enterprise information security requirements.	• Number of key security roles clearly defined • Number of security related incidents
2. A security plan has been established, accepted and communicated throughout the enterprise.	• Level of stakeholder satisfaction with the security plan throughout the enterprise • Number of security solutions deviating from the plan • Number of security solutions deviating from the enterprise architecture
3. Information security solutions are implemented and operated consistently throughout the enterprise.	• Number of services with confirmed alignment to the security plan • Number of security incidents caused by non-adherence to the security plan • Number of solutions developed with confirmed alignment to the security plan

APO13 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
APO13.01 Establish and maintain an ISMS.		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02 Define and manage an information security risk treatment plan.		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03 Monitor and review the ISMS.					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

APO13 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO13.01 Establish and maintain an information security management system (ISMS). Establish and maintain an ISMS that provides a standard, formal and continuous approach to security management for information, enabling secure technology and business processes that are aligned with business requirements and enterprise security management.	Outside COBIT	Enterprise security approach	ISMS policy	Internal
			ISMS scope statement	APO01.02 DSS06.03

Activities
1. Define the scope and boundaries of the ISMS in terms of the characteristics of the enterprise, the organisation, its location, assets and technology. Include details of, and justification for, any exclusions from the scope.
2. Define an ISMS in accordance with enterprise policy and aligned with the enterprise, the organisation, its location, assets and technology.
3. Align the ISMS with the overall enterprise approach to the management of security.
4. Obtain management authorisation 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.

APO13 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO13.02 Define and manage an information security risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with the enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases and implemented as an integral part of services and solutions development, then operated as an integral part of business operation.	**From**	**Description**	**Description**	**To**
	APO02.04	Gaps and changes required to realise target capability	Information security risk treatment plan	All EDM All APO All BAI All DSS All MEA
	APO03.02	Baseline domain descriptions and architecture definition	Information security business cases	APO02.05
	APO12.05	Project proposals for reducing risk		
Activities				
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.				
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, which 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. Define how to measure the effectiveness of the selected management practices and specify how these measurements are to be used to assess effectiveness to produce comparable and reproducible results.				
6. Recommend information security training and awareness programmes.				
7. Integrate the planning, design, implementation and monitoring of information security procedures and other controls capable of enabling prompt prevention, detection of security events and response to security incidents.				
Management Practice	**Inputs**		**Outputs**	
APO13.03 Monitor and review the ISMS. Maintain and regularly communicate the need for, and benefits of, continuous information security improvement. Collect and analyse data about the ISMS, and improve the effectiveness of the ISMS. Correct non-conformities to prevent recurrence. Promote a culture of security and continual improvement.	**From**	**Description**	**Description**	**To**
	DSS02.02	Classified and prioritised incidents and service requests	ISMS audit reports	MEA02.01
			Recommendations for improving the ISMS	Internal
Activities				
1. Undertake regular reviews of the effectiveness of the ISMS including meeting ISMS policy and objectives, and review of security practices. Take into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.				
2. Conduct internal 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. Provide input to the maintenance of the security plans to take into account the findings of monitoring and reviewing activities.				
5. Record actions and events that could have an impact on the effectiveness or performance of the ISMS.				

APO13 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 27001:2005	Information security management systems—Requirements, Section 4
ISO/IEC 27002:2011	
National Institute of Standards and Technology (NIST) SP800-53 Rev 1	Recommended Security Controls for USA Federal Information Systems