A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	9.3 Release and deployment management
ITIL V3 2011	Service Transition, 4.4 Release and Deployment Management
Management Practice	**Example Metrics**
BAI07.07 Provide early production support. For an agreed period of time, provide early support to users and I&T operations to resolve issues and help stabilize the new solution.	a. Number of additional I&T system resources provided for support b. Number of additional staff resources provided for support
Activities	**Capability Level**
1. Provide additional resources, as required, to end users and support personnel until the release has stabilized.	3
2. Provide additional I&T systems resources, as required, until the release is in a stable operational environment.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI07.08 Perform a post-implementation review. Conduct a post-implementation review to confirm outcome and results, identify lessons learned, and develop an action plan. Evaluate actual performance and outcomes of the new or changed service against expected performance and outcomes anticipated by the user or customer.	a. Number and percent of root cause analyses completed b. Number or percent of releases that fail to stabilize within an acceptable period c. Percent of releases causing downtime
Activities	**Capability Level**
1. Establish procedures to ensure that post-implementation reviews identify, assess and report on the extent to which the following events have occurred: enterprise requirements have been met; expected benefits have been realized; the system is considered usable; internal and external stakeholder expectations are met; unexpected impacts on the enterprise have occurred; key risk is mitigated; and the change management, installation and accreditation processes were performed effectively and efficiently.	3
2. Consult business process owners and IT technical management in the choice of metrics for measurement of success and achievement of requirements and benefits.	4
3. Conduct the post-implementation review in accordance with the organizational change management process. Engage business process owners and third parties, as appropriate.	
4. Consider requirements for post-implementation review arising from outside business and IT (e.g., internal audit, ERM, compliance).	
5. Agree on and implement an action plan to address issues identified in the post-implementation review. Engage business process owners and IT technical management in the development of the action plan.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Transition, 4.6 Change Evaluation

B. Component: Organizational Structures									
Key Management Practice	Chief Information Officer	Business Process Owners	Data Management Function	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI07.01 Establish an implementation plan.	A	R		R		R	R	R	
BAI07.02 Plan business process, system and data conversion.	A	R	R	R		R	R	R	
BAI07.03 Plan acceptance tests.	A	R		R	R		R	R	R
BAI07.04 Establish a test environment.	A	R		R	R		R	R	
BAI07.05 Perform acceptance tests.	A	R		R	R		R	R	R
BAI07.06 Promote to production and manage releases.	A	R		R	R	R		R	
BAI07.07 Provide early production support.	A	R		R	R	R			
BAI07.08 Perform a post-implementation review.	A	R		R	R	R			

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI07.01 Establish an implementation plan.	BAI01.07	Quality management plan	Implementation fallback and recovery processes	Internal
	BAI06.01	• Approved requests for change • Change plan and schedule	Approved implementation plan	Internal
	BAI11.05	Project quality management plan		
BAI07.02 Plan business process, system and data conversion.			Migration plan	DSS06.02
BAI07.03 Plan acceptance tests.	BAI01.07	Requirements for independent verification of deliverables	Approved acceptance test plan	BAI01.04; BAI11.04
	BAI03.07	• Test plan • Test procedures		
	BAI03.08	• Test result logs and audit trails • Test result communications		
	BAI11.05	Requirements for independent verification of project deliverables		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI07.04 Establish a test environment.	**From**	**Description**	**Description**	**To**
			Test data	Internal
BAI07.05 Perform acceptance tests.			Approved acceptance and release for production	BAI01.04
			Evaluation of acceptance results	BAI01.06
			Test results log	Internal
BAI07.06 Promote to production and manage releases.			Release plan	BAI10.01
			Release log	Internal
BAI07.07 Provide early production support.	APO11.02	Results of quality of service, including customer feedback	Supplemental support plan	APO08.04; APO08.05; DSS02.04
	BAI05.05	Success measures and results		
BAI07.08 Perform a post-implementation review.	APO11.03	• Results of solution and service delivery quality monitoring • Root causes of quality delivery failures	Remedial action plan	BAI01.09; BAI11.09
	APO11.04	Results of quality reviews and audits	Post-implementation review report	BAI01.09; BAI11.09
	BAI05.05	Success measures and results		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business process testing	Skills Framework for the Information Age V6, 2015	BPTS
Release and deployment	Skills Framework for the Information Age V6, 2015	RELM
Service acceptance	Skills Framework for the Information Age V6, 2015	SEAC
Testing	Skills Framework for the Information Age V6, 2015	TEST
User experience evaluation	Skills Framework for the Information Age V6, 2015	USEV

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
IT change management policy	Communicates management intent that all changes to enterprise IT are managed and implemented so as to minimize risk and impact to stakeholders. Covers in-scope assets and standard change management process.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture that ensures timely communication of IT change requests to affected groups; consult the affected groups regarding implementation and testing of changes.		

G. Component: Services, Infrastructure and Applications
• IT change management tools • Release management tools • Testing tools and services

Domain: Build, Acquire and Implement Management Objective: BAI08 — Managed Knowledge	Focus Area: COBIT Core Model

Description

Maintain the availability of relevant, current, validated and reliable knowledge and management information to support all process activities and to facilitate decision making related to the governance and management of enterprise I&T. Plan for the identification, gathering, organizing, maintaining, use and retirement of knowledge.

Purpose

Provide the knowledge and information required to support all staff in the governance and management of enterprise I&T and allow for informed decision making.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG10 Staff skills, motivation and productivity • EG13 Product and business innovation	• AG12 Competent and motivated staff with mutual understanding of technology and business • AG13 Knowledge, expertise and initiatives for business innovation

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG12	a. Percent of I&T-savvy business people (i.e., those having the required knowledge and understanding of I&T to guide, direct, innovate and see I&T opportunities in their domain of business expertise) b. Percent of business-savvy I&T people (i.e., those having the required knowledge and understanding of relevant business domains to guide, direct, innovate and see I&T opportunities for the business domain) c. Number or percentage of business people with technology management experience
EG10	a. Staff productivity compared to benchmarks b. Level of stakeholder satisfaction with staff expertise and skills c. Percent of staff whose skills are insufficient for competency in their role d. Percent of satisfied staff	AG13	a. Level of business executive awareness and understanding of I&T innovation possibilities b. Number of approved initiatives resulting from innovative I&T ideas c. Number of innovation champions recognized/awarded
EG13	a. Level of awareness and understanding of business innovation opportunities b. Stakeholder satisfaction with levels of product and innovation expertise and ideas c. Number of approved product and service initiatives resulting from innovative ideas		

A. Component: Process	
Management Practice	**Example Metrics**
BAI08.01 Identify and classify sources of information for governance and management of I&T. Identify, validate and classify diverse sources of internal and external information required to enable governance and management of I&T, including strategy documents, incident reports and configuration information that progresses from development to operations before going live.	a. Percent of categorized information validated b. Percent of appropriateness of content types, artifacts, and structured and unstructured information

Activities	Capability Level
1. Identify potential knowledge users, including owners of information who may need to contribute and approve knowledge. Obtain knowledge requirements and sources of information from identified users.	2
2. Consider content types (procedures, processes, structures, concepts, policies, rules, facts, classifications), artefacts (documents, records, video, voice), and structured and unstructured information (experts, social media, email, voice mail, Rich Site Summary (RSS) feeds).	
3. Classify sources of information based on a content classification scheme (e.g., information architecture model). Map sources of information to the classification scheme.	3
4. Collect, collate and validate information sources based on information validation criteria (e.g., understandability, relevance, importance, integrity, accuracy, consistency, confidentiality, currency and reliability).	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
BAI08.02 Organize and contextualize information into knowledge. Organize information based on classification criteria. Identify and create meaningful relationships among information elements and enable use of information. Identify owners, and leverage and implement enterprise-defined information levels of access to management information and knowledge resources.	a. Number of relationships identified among sources of information (tagging) b. Percent of stakeholder satisfaction with the organization and contextualization of information into knowledge

Activities	Capability Level
1. Identify shared attributes and match sources of information, creating relationships among information sets (information tagging).	3
2. Create views to related data sets, considering stakeholder and organizational requirements.	
3. Devise and implement a scheme to manage unstructured knowledge not available through formal sources (e.g., expert knowledge).	
4. Publish and make knowledge accessible to relevant stakeholders, based on roles and access mechanisms.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting - Principle 18

Management Practice	Example Metrics
BAI08.03 Use and share knowledge. Propagate available knowledge resources to relevant stakeholders and communicate how these resources can be used to address different needs (e.g., problem solving, learning, strategic planning and decision making).	a. Percent of available knowledge actually used b. Percent of knowledge user satisfaction

Activities	Capability Level
1. Set management expectations and demonstrate appropriate attitude regarding the usefulness of knowledge and the need to share knowledge related to the governance and management of enterprise I&T.	2
2. Identify potential knowledge users by knowledge classification.	
3. Transfer knowledge to knowledge users, based on a needs gap analysis and effective learning techniques. Create an environment, tools and artifacts that support the sharing and transfer of knowledge. Ensure appropriate access controls are in place, in line with defined knowledge classification.	3
4 .Measure the use of knowledge tools and elements and evaluate the impact on governance processes.	4
5. Improve information and knowledge for governance processes that show knowledge gaps.	5

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	PP.IS Apply Information Sharing; IR.ES Ensure Information sharing
ITIL V3, 2011	Service Transition, 4.7 Knowledge Management
PMBOK Guide Sixth Edition, 2017	Part 1: 4.4 Manage project knowledge
Management Practice	**Example Metrics**
BAI08.04 Evaluate and update or retire information. Measure the use and evaluate the currency and relevance of information. Update information or retire obsolete information.	a. Frequency of update b. Level of satisfaction of users

Activities	Capability Level
1. Define the controls for knowledge retirement and retire knowledge accordingly.	3
2. Evaluate the usefulness, relevance and value of knowledge elements. Update outdated information that still has relevance and value to the organization. Identify related information that is no longer relevant to the enterprise's knowledge requirements and retire or archive according to policy.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures																		
Key Management Practice	**Chief Information Officer**	**Chief Technology Officer**	**Chief Digital Officer**	**Business Process Owners**	**Portfolio Manager**	**Program Manager**	**Project Manager**	**Data Management Function**	**Head Architect**	**Head Development**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Business Continuity Manager**	**Privacy Officer**	**Legal Counsel**
BAI08.01 Identify and classify sources of information for governance and management of I&T.	A			R				R		R	R		R				
BAI08.02 Organize and contextualize information into knowledge.	A							R		R	R	R					
BAI08.03 Use and share knowledge.	A	R	R	R	R	R	R	R				R					R
BAI08.04 Evaluate and update or retire information.	A			R		R	R	R	R	R	R	R	R	R	R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI08.01 Identify and classify sources of information for governance and management of I&T.	Outside COBIT	Knowledge requirements and sources	Classification of information sources	Internal
BAI08.02 Organize and contextualize information into knowledge.	BAI03.03	Documented solution components	Published knowledge repositories	APO07.03
	BAI05.07	Knowledge transfer plans		
BAI08.03 Use and share knowledge.	BAI03.03	Documented solution components	Knowledge awareness and training schemes	APO07.03
	BAI05.05	Operation and use plan	Knowledge user database	Internal
	BAI05.07	Knowledge transfer plans		
BAI08.04 Evaluate and update or retire information.			Rules for knowledge retirement	Internal
			Knowledge use evaluation results	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Information and knowledge management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.10. Information and Knowledge Management

E. Component: Policies and Procedures			
Relevant Policy	Policy Description	Related Guidance	Detailed Reference
Governance knowledge use policy	Guides creation and use of knowledge assets relating to I&T governance. I&T knowledge assets should be readily accessible for reference.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	Related Guidance	Detailed Reference
Embed a knowledge-sharing culture in the enterprise. Proactively communicate the value of knowledge to encourage knowledge creation, use, reuse and sharing. Encourage the sharing and transfer of knowledge by identifying and leveraging motivational factors.		

G. Component: Services, Infrastructure and Applications
• Collaboration platform • Knowledge repository

Domain: Build, Acquire and Implement Management Objective: BAI09 — Managed Assets	Focus Area: COBIT Core Model

Description

Manage I&T assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected. Ensure that those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements.

Purpose

Account for all I&T assets and optimize the value provided by their use.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG04 Quality of financial information • EG07 Quality of management information • EG09 Optimization of business process costs	AG04 Quality of technology-related financial information

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG04	a. Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information b. Cost of noncompliance with finance-related regulations	AG04	a. Satisfaction of key stakeholders regarding the level of transparency, understanding and accuracy of I&T financial information b. Percent of I&T services with defined and approved operational costs and expected benefits
EG07	a. Degree of board and executive management satisfaction with decision-making information b. Number of incidents caused by incorrect business decisions based on inaccurate information c. Time to provide information supporting effective business decisions d. Timeliness of management information		
EG09	a. Ratio of cost vs. achieved service levels b. Satisfaction levels of board and executive management with business processing costs		

A. Component: Process

Management Practice	Example Metrics
BAI09.01 Identify and record current assets. Maintain an up-to-date, accurate record of all I&T assets that are required to deliver services and that are owned or controlled by the organization with an expectation of future benefit (including resources with economic value, such as hardware or software). Ensure alignment with configuration management and financial management.	a. Percent of assets accurately recorded in asset register b. Percent of assets that are fit for purpose c. Percent of assets inventoried and kept current

Activities	Capability Level
1. Identify all owned assets in an asset register that records current status. Assets are reported on the balance sheet; they are bought or created to increase the value of a firm or benefit the enterprise's operations (e.g., hardware and software). Identify all owned assets and maintain alignment with the change management and configuration management processes, the configuration management system, and the financial accounting records.	2
2. Identify legal, regulatory or contractual requirements that need to be addressed when managing the asset.	
3. Verify that the assets are fit for purpose (i.e., in a useful condition).	
4. Ensure accounting for all assets.	3
5. Verify the existence of all owned assets by performing regular physical and logical inventory checks and reconciliation. Include the use of software discovery tools.	4
6. Determine on a regular basis whether each asset continues to provide value. If so, estimate the expected useful life for delivering value.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RI.AD Asset Discovery & Identification
ISF, The Standard of Good Practice for Information Security 2016	BA1.1 Business Application Register
ISO/IEC 27002:2013/Cor.2:2015(E)	8.1 Responsibility for assets
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.13 Physical and environmental protection (PE-9)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software
Management Practice	**Example Metrics**
BAI09.02 Manage critical assets. Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs.	a. Number of critical assets b. Average downtime per critical asset c. Number of incident trends identified

Activities	Capability Level
1. Identify assets that are critical in providing service capability by referencing requirements in service definitions, SLAs and the configuration management system.	2
2. On a regular basis, consider the risk of failure or need for replacement of each critical asset.	
3. Communicate to affected customers and users the expected impact (e.g., performance restrictions) of maintenance activities.	
4. Incorporate planned downtime in an overall production schedule. Schedule the maintenance activities to minimize the adverse impact on business processes.	3
5. Maintain the resilience of critical assets by applying regular preventive maintenance. Monitor performance and, if required, provide alternative and/or additional assets to minimize the likelihood of failure.	
6. Establish a preventive maintenance plan for all hardware, considering cost/benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors.	
7. Establish maintenance agreements involving third-party access to organizational I&T facilities for on-site and off-site activities (e.g., outsourcing). Establish formal service contracts containing or referring to all necessary security and privacy conditions, including access authorization procedures, to ensure compliance with the organizational security/privacy policies and standards.	
8. Ensure that remote access services and user profiles (or other means used for maintenance or diagnosis) are active only when required.	
9. Monitor performance of critical assets by examining incident trends. Where necessary, take action to repair or replace.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.AM Asset Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.13 Physical and environmental protection (PE-20)
Management Practice	**Example Metrics**
BAI09.03 Manage the asset life cycle. Manage assets from procurement to disposal. Ensure that assets are utilized as effectively and efficiently as possible and are accounted for and physically protected until appropriately retired.	a. Percent of assets managed from procurement to disposal b. Utilization percentage per asset c. Percent of assets deployed following the standard implementation life cycle

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Procure all assets based on approved requests and in accordance with the enterprise procurement policies and practices.	2
2. Source, receive, verify, test and record all assets in a controlled manner, including physical labeling as required.	
3. Approve payments and complete the process with suppliers according to agreed contract conditions.	
4. Deploy assets following the standard implementation life cycle, including change management and acceptance testing.	3
5. Allocate assets to users, with acceptance of responsibilities and sign-off, as appropriate.	
6. Whenever possible, reallocate assets when they are no longer required due to a change of user role, redundancy within a service, or retirement of a service.	
7. Plan, authorize and implement retirement-related activities, retaining appropriate records to meet ongoing business and regulatory needs.	
8. Dispose of assets securely, considering, for example, the permanent deletion of any recorded data on media devices and potential damage to the environment.	
9. Dispose of assets responsibly when they serve no useful purpose due to retirement of all related services, obsolete technology or lack of users with regard to environmental impact.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	DP.ML Manage Asset Lifecycle
ISF, The Standard of Good Practice for Information Security 2016	IM2.1 Document Management; PA1.1 Hardware Life Cycle Management
ITIL V3, 2011	Service Transition, 4.3 Service Asset and Configuration Management
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	PR.MA Maintenance
Management Practice	**Example Metrics**
BAI09.04 Optimize asset value. Regularly review the overall asset base to identify ways to optimize value in alignment with business needs.	a. Benchmark costs b. Number of assets not utilized
Activities	**Capability Level**
1. On a regular basis, review the overall asset base, considering whether it is aligned with business requirements.	3
2. Assess maintenance costs, consider reasonableness, and identify lower-cost options. Include, where necessary, replacement with new alternatives.	4
3. Review warranties and consider value-for-money and replacement strategies to determine lowest-cost options.	5
4. Use capacity and utilization statistics to identify underutilized or redundant assets that could be considered for disposal or replacement to reduce costs.	
5. Review the overall base to identify opportunities for standardization, single sourcing, and other strategies that may lower procurement, support and maintenance costs.	
6. Review the overall state to identify opportunities to leverage emerging technologies or alternative sourcing strategies to reduce costs or increase value-for-money.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI09.05 Manage licenses. Manage software licenses to maintain the optimal number of licenses and support business requirements. Ensure that the number of licenses owned is sufficient to cover the installed software in use.	a. Percent of used licenses against purchased licenses b. Percent of licenses still being paid for but not being used c. Percent of products and licenses that should be upgraded to achieve better value

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Maintain a register of all purchased software licenses and associated license agreements.	2
2. On a regular basis, conduct an audit to identify all instances of installed licensed software.	3
3. Compare the number of installed software instances with the number of licenses owned. Ensure that the license compliance measurement method is compliant with the license and contractual requirements.	4
4. When instances are lower than the number owned, decide whether there is a need to retain or terminate licenses, considering the potential to save on unnecessary maintenance, training and other costs.	
5. When instances are higher than the number owned, consider first the opportunity to uninstall instances that are no longer required or justified, and then, if necessary, purchase additional licenses to comply with the license agreement.	
6. On a regular basis, consider whether better value can be obtained by upgrading products and associated licenses.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures									
Key Management Practice	**Chief Information Officer**	**Chief Technology Officer**	**Head Architect**	**Head Development**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Privacy Officer**
BAI09.01 Identify and record current assets.		A			R	R			
BAI09.02 Manage critical assets.		A	R	R	R	R		R	R
BAI09.03 Manage the asset life cycle.		A			R	R	R		
BAI09.04 Optimize asset value.	A	R	R	R	R	R	R		
BAI09.05 Manage licenses.	A	R		R	R	R			
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**								
No related guidance for this component									

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
BAI09.01 Identify and record current assets.	**From**	**Description**	**Description**	**To**
	BAI03.04	Updates to asset inventory	Results of fit-for-purpose reviews	APO02.02
	BAI10.02	Configuration repository	Asset register	APO06.01; BAI10.03
			Results of physical inventory checks	BAI10.03; BAI10.04; DSS05.03
BAI09.02 Manage critical assets.			Communications of planned maintenance downtime	APO08.04
			Maintenance agreements	Internal
BAI09.03 Manage the asset life cycle.			Authorized asset retirements	BAI10.03
			Updated asset register	BAI10.03
			Approved asset procurement requests	Internal
BAI09.04 Optimize asset value.			Opportunities to reduce asset costs or increase value	APO02.02
			Results of cost-optimization reviews	APO02.02
BAI09.05 Manage licenses.			Action plan to adjust license numbers and allocations	APO02.05
			Register of software licenses	BAI10.02
			Results of installed license audits	MEA03.03
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Asset management	Skills Framework for the Information Age V6, 2015	ASMG
Systems installation/ decommissioning	Skills Framework for the Information Age V6, 2015	HSIN

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Asset management policy	Provides guidelines for asset life cycle management, asset protection measures, system classification and ownership, data ownership, and data classification		
Intellectual property (IP) policy	Addresses risk related to use, ownership, sale and distribution of the outputs of I&T-related creative endeavors by employees (e.g., software development). Mandates appropriate documentation, level of detail, etc., from inception of work.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture that identifies, assesses, and reports the relative economic and strategic value of each asset to the enterprise in an open, consistent and transparent manner.		

G. Component: Services, Infrastructure and Applications
Asset management tools

Domain: Build, Acquire and Implement Management Objective: BAI10 — Managed Configuration	Focus Area: COBIT Core Model

Description

Define and maintain descriptions and relationships among key resources and capabilities required to deliver I&T-enabled services. Include collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.

Purpose

Provide sufficient information about service assets to enable the service to be effectively managed. Assess the impact of changes and deal with service incidents.

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
BAI10.01 Establish and maintain a configuration model. Establish and maintain a logical model of the services, assets, infrastructure and recording of configuration items (CIs), including the relationships among them. Include the CIs considered necessary to manage services effectively and to provide a single, reliable description of the assets in a service.	a. Number of stakeholders signing off on the configuration model b. Percent of accuracy of relationships of configuration items

Activities	Capability Level
1. Define and agree on the scope and level of detail for configuration management (i.e., which services, assets and infrastructure configurable items to include).	3
2. Establish and maintain a logical model for configuration management, including information on CI types, attributes, relationship types, relationship attributes and status codes.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes - Configuration Management
ISF, The Standard of Good Practice for Information Security 2016	SY1 System Configuration
ISO/IEC 20000-1:2011(E)	9.1 Configuration management
ITIL V3, 2011	Service Transition, 4.3 Service Asset and Configuration Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-6)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI10.02 Establish and maintain a configuration repository and baseline. Establish and maintain a configuration management repository and create controlled configuration baselines.	a. Number of configuration items (CIs) listed in the repository b. Percent of accuracy of configuration baselines of a service, application or infrastructure
Activities	**Capability Level**
1. Identify and classify CIs and populate the repository.	2
2. Create, review and formally agree on configuration baselines of a service, application or infrastructure.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.CB Apply Configuration Baselines
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.4 Implementation (Task 2)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.19 System and service acquisition (SA-10)
Management Practice	**Example Metrics**
BAI10.03 Maintain and control configuration items. Maintain an up-to-date repository of configuration items (CIs) by populating any configuration changes.	a. Frequency of changes/updates to the repository b. Percent of accuracy and completeness of CIs repository
Activities	**Capability Level**
1. Regularly identify all changes to CIs.	2
2. To ensure completeness and accuracy, review proposed changes to CIs against the baseline.	
3. Update configuration details for approved changes to CIs.	
4. Create, review and formally agree on changes to configuration baselines whenever needed.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-2)
Management Practice	**Example Metrics**
BAI10.04 Produce status and configuration reports. Define and produce configuration reports on status changes of configuration items.	a. Number of identified unauthorized changes b. Percent of accuracy of status changes of CIs against the baseline
Activities	**Capability Level**
1. Identify status changes of CIs and report against the baseline.	2
2. Match all configuration changes with approved requests for change to identify any unauthorized changes. Report unauthorized changes to change management.	3
3. Identify reporting requirements from all stakeholders, including content, frequency and media. Produce reports according to the identified requirements.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-3)
Management Practice	**Example Metrics**
BAI10.05 Verify and review integrity of the configuration repository. Periodically review the configuration repository and verify completeness and correctness against the desired target.	a. Number of deviations between the configuration repository and live configuration b. Number of discrepancies relating to incomplete or missing configuration information

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Periodically verify live configuration items against the configuration repository by comparing physical and logical configurations and using appropriate discovery tools, as required.	4
2. Report and review all deviations for approved corrections or action to remove any unauthorized assets.	
3. Periodically verify that all physical configuration items, as defined in the repository, physically exist. Report any deviations to management.	
4. Set and periodically review the target for completeness of the configuration repository based on business need.	
5. Periodically compare the degree of completeness and accuracy against targets and take remedial action, as necessary, to improve the quality of the repository data.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-4)

B. Component: Organizational Structures									
Key Management Practice	**Chief Information Officer**	**Chief Technology Officer**	**Head Architect**	**Head Development**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	
BAI10.01 Establish and maintain a configuration model.		A			R	R	R		
BAI10.02 Establish and maintain a configuration repository and baseline.		A		R	R	R	R	R	
BAI10.03 Maintain and control configuration items.	A	R		R	R	R			
BAI10.04 Produce status and configuration reports.		A			R	R			
BAI10.05 Verify and review integrity of the configuration repository.		A	R	R	R		R		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
BAI10.01 Establish and maintain a configuration model.	**From**	**Description**	**Description**	**To**
	BAI07.06	Release plan	Logical configuration model	Internal
			Scope of configuration management model	Internal
BAI10.02 Establish and maintain a configuration repository and baseline.	BAI09.05	Register of software licenses	Configuration baseline	BAI03.11; BAI03.12
			Configuration repository	BAI09.01; DSS02.01
BAI10.03 Maintain and control configuration items.	BAI06.03	Change request status reports	Approved changes to baseline	BAI03.11
	BAI09.01	• Asset register • Results of physical inventory checks	Updated repository with CIs	DSS02.01
	BAI09.03	• Updated asset register • Authorized asset retirements		
BAI10.04 Produce status and configuration reports.	BAI09.01	Results of physical inventory checks	Configuration status reports	BAI03.11; DSS02.01
BAI10.05 Verify and review integrity of the configuration repository.			Results of repository completeness reviews	Internal
			Results of physical verification of CIs	Internal
			License deviations	MEA03.03
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.4 Implementation (Task 2): Inputs and Outputs			

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Configuration management	Skills Framework for the Information Age V6, 2015	CFMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Configuration management policy	Communicates guidance for establishing and using a comprehensive configuration repository, including all technology components, associated configuration definitions and interdependencies with other technology components. Helps ensure that system and software changes are minimally disruptive to services. Ensures that changes are coordinated among applicable groups, so conflicts or duplication of effort do not occur.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture that supports a structured approach to configuration management across departments in which users recognize the value of strict configuration management (e.g., avoiding version conflicts or duplicative effort) and apply the rules and procedures that were put in place.		

G. Component: Services, Infrastructure and Applications
Configuration management tools and repositories

Page intentionally left blank

Domain: Build, Acquire and Implement Management objective: BAI11 — Managed Projects	Focus Area: COBIT Core Model

Description

Manage all projects that are initiated within the enterprise in alignment with enterprise strategy and in a coordinated way based on the standard project management approach. Initiate, plan, control and execute projects, and close with a post-implementation review.

Purpose

Realize defined project outcomes and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end users. Ensure the value and quality of project deliverables and maximize their contribution to the defined programs and investment portfolio.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	• AG03 Realized benefits from I&T-enabled investments and services portfolio • AG06 Agility to turn business requirements into operational solutions • AG09 Delivering programs on time, on budget and meeting requirements and quality standards

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG03	a. Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded b. Percent of I&T services for which expected benefits (as stated in service level agreements) are realized
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	AG06	a. Level of satisfaction of business executives with I&T responsiveness to new requirements b. Average time to market for new I&T-related services and applications c. Average time to turn strategic I&T objectives into agreed and approved initiatives d. Number of critical business processes supported by up-to-date infrastructure and applications
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates	AG09	a. Number of programs/projects on time and within budget b. Number of programs needing significant rework due to quality defects c. Percent of stakeholders satisfied with program/project quality

A. Component: Process	
Management Practice	**Example Metrics**
BAI11.01 Maintain a standard approach for project management. Maintain a standard approach for project management that enables governance and management review, decision-making and delivery-management activities. These activities should focus consistently on business value and goals (i.e., requirements, risk, costs, schedule and quality targets).	a. Percent of successful projects based on the defined standard approach b. Number of updates to project management approach, good practices, tools and templates

Activities	Capability Level
1. Maintain and enforce a standard approach to project management aligned to the enterprise's specific environment and with good practice based on defined process and use of appropriate technology. Ensure that the approach covers the full life cycle and disciplines to be followed, including the management of scope, resources, risk, cost, quality, time, communication, stakeholder involvement, procurement, change control, integration and benefit realization.	2
2. Provide appropriate project management training and consider certification for project managers.	
3. Put in place a project management office (PMO) that maintains the standard approach for program and project management across the organization. The PMO supports all projects by creating and maintaining required project documentation templates, providing training and best practices for project managers, tracking metrics on the use of best practices for project management, etc. In some cases, the PMO may also report on project progress to senior management and/or stakeholders, help prioritize projects, and ensure all projects support the overall business objectives of the enterprise.	3
4. Evaluate lessons learned on the use of the project management approach. Update the good practices, tools and templates accordingly.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-2)

Management Practice	Example Metrics
BAI11.02 Start up and initiate a project. Define and document the nature and scope of the project to confirm and develop a common understanding of project scope among stakeholders. The definition should be formally approved by the project sponsors.	a. Percent of stakeholders approving enterprise need, scope, planned outcome and level of project risk b. Percent of projects in which stakeholders received a clear written statement defining the nature, scope and benefit of the project

Activities	Capability Level
1. To create a common understanding of project scope among stakeholders, provide them a clear written statement defining the nature, scope and deliverables of every project.	2
2. Ensure that each project has one or more sponsors with sufficient authority to manage execution of the project within the overall program.	
3. Ensure that key stakeholders and sponsors within the enterprise (business and IT) agree on and accept the requirements for the project, including definition of project success (acceptance) criteria and key performance indicators (KPIs).	
4. Appoint a dedicated manager for the project. Ensure that the individual has the required understanding of technology and business and the commensurate competencies and skills to manage the project effectively and efficiently.	
5. Ensure that the project definition describes the requirements for a project communication plan that identifies internal and external project communications.	
6. With the approval of stakeholders, maintain the project definition throughout the project, reflecting changing requirements.	
7. To track the execution of a project, put in place mechanisms such as regular reporting and stage-gate, release or phase reviews, to occur in a timely manner and with appropriate approval.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 4.1 Develop project charter; Part 1: 6. Project schedule management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI11.03 Manage stakeholder engagement. Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information that reaches all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	a. Level of stakeholder satisfaction with involvement b. Percent of stakeholders effectively engaged
Activities	**Capability Level**
1. Plan how stakeholders inside and outside the enterprise will be identified, analyzed, engaged and managed through the life cycle of the project.	3
2. Identify, engage and manage stakeholders by establishing and maintaining appropriate levels of co-ordination, communication and liaison to ensure they are involved in the project.	
3. Analyze stakeholder interests, requirements and engagement. Take remedial actions as required.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 13. Project stakeholder management Part 1: 10. Project communications management
Management Practice	**Example Metrics**
BAI11.04 Develop and maintain the project plan. Establish and maintain a formal, approved, integrated project plan (covering business and IT resources) to guide project execution and control throughout the life of the project. The scope of projects should be clearly defined and tied to building or enhancing business capability.	a. Percent of active projects undertaken without valid and updated project value maps b. Percent of milestone or task completion vs. plan
Activities	**Capability Level**
1. Develop a project plan that provides information to enable management to control project progress progressively. The plan should include details of project deliverables and acceptance criteria, required internal and external resources and responsibilities, clear work breakdown structures and work packages, estimates of resources required, milestones/release plan/phases, key dependencies, budget and costs, and identification of a critical path.	2
2. Maintain the project plan and any dependent plans (e.g., risk plan, quality plan, benefits realization plan). Ensure that the plans are up to date and reflect actual progress and approved material changes.	
3. Ensure that there is effective communication of project plans and progress reports. Ensure that any changes made to individual plans are reflected in other plans.	
4. Determine the activities, interdependencies and required collaboration and communication within the project and among multiple projects within a program.	
5. Ensure that each milestone is accompanied by a significant deliverable requiring review and sign-off.	
6. Establish a project baseline (e.g., cost, schedule, scope, quality) that is appropriately reviewed, approved and incorporated into the integrated project plan.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.2 Develop project management plan
Management Practice	**Example Metrics**
BAI11.05 Manage project quality. Prepare and execute a quality management plan, processes and practices that align with quality management standards (QMS). Describe the approach to project quality and implementation. The plan should be formally reviewed and agreed on by all parties concerned and incorporated into the integrated project plans.	a. Percent of build-to-products without errors b. Number of cancelled projects

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. To provide quality assurance for the project deliverables, identify ownership and responsibilities, quality review processes, success criteria and performance metrics.	2
2. Identify assurance tasks and practices required to support the accreditation of new or modified systems during project planning. Include them in the integrated plans. Ensure that the tasks provide assurance that internal controls and security and privacy solutions meet the defined requirements.	3
3. Define any requirements for independent validation and verification of the quality of deliverables in the plan.	
4. Perform quality assurance and control activities in accordance with the quality management plan and QMS.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8. Project quality management
Management Practice	**Example Metrics**
BAI11.06 Manage project risk. Eliminate or minimize specific risk associated with projects through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with potential to cause unwanted change. Define and record any risk faced by project management.	a. Number of identified delays and issues b. Number of projects with a formal project risk management approach aligned with the ERM framework
Activities	**Capability Level**
1. Establish a formal project risk management approach aligned with the ERM framework. Ensure that the approach includes identifying, analyzing, responding to, mitigating, monitoring and controlling risk.	2
2. Assign to appropriately skilled personnel the responsibility for executing the enterprise's project risk management process within a project and ensure that this is incorporated into the solution development practices. Consider allocating this role to an independent team, especially if an objective viewpoint is required or a project is considered critical.	
3. Identify owners for actions to avoid, accept or mitigate risk.	
4. Perform the project risk assessment of identifying and quantifying risk continuously throughout the project. Manage and communicate risk appropriately within the project governance structure.	3
5. Reassess project risk periodically, including at initiation of each major project phase and as part of major change request assessments.	
6. Maintain and review a project risk register of all potential project risk and a risk mitigation log of all project issues and their resolution. Analyze the log periodically for trends and recurring problems to ensure that root causes are corrected.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-4)
PMBOK Guide Sixth Edition, 2017	Part 1: 11. Project risk management
Management Practice	**Example Metrics**
BAI11.07 Monitor and control projects. Measure project performance against key project performance criteria such as schedule, quality, cost and risk. Identify any deviations from expected targets. Assess the impact of deviations on the project and overall program and report results to key stakeholders.	a. Percent of activities aligned to scope and expected outcomes b. Percent of deviations from plan addressed c. Frequency of project status reviews

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Establish and use a set of project criteria including, but not limited to, scope, expected business benefit, schedule, quality, cost and level of risk.	2
2. Report to identified key stakeholders project progress within the project, deviations from established key project performance criteria (such as, but not limited to, the expected business benefits), and potential positive and negative effects on the project.	
3. Document and submit any necessary changes to the project's key stakeholders for their approval before adoption. Communicate revised criteria to project managers for use in future performance reports.	
4. For the deliverables produced in each iteration, release or project phase, gain approval and sign-off from designated managers and users in the affected business and IT functions.	
5. Base the approval process on clearly defined acceptance criteria agreed on by key stakeholders before work commences on the project phase or iteration deliverable.	3
6. Assess the project at agreed major stage-gates, releases or iterations. Make formal go/no-go decisions based on predetermined critical success criteria.	
7. Establish and operate a change control system for the project so that all changes to the project baseline (e.g., scope, expected business benefits, schedule, quality, cost, risk level) are appropriately reviewed, approved and incorporated into the integrated project plan in line with the program and project governance framework.	
8. Measure project performance against key project performance criteria. Analyze deviations from established key project performance criteria for cause and assess positive and negative effects on the project.	4
9. Monitor changes to the project and review existing key project performance criteria to determine whether they still represent valid measures of progress.	
10. Recommend and monitor remedial action, when required, in line with the project governance framework.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.5 Monitor and control project work
Management Practice	**Example Metrics**
BAI11.08 Manage project resources and work packages. Manage project work packages by placing formal requirements on authorizing and accepting work packages and assigning and coordinating appropriate business and IT resources.	a. Number of resource issues (e.g., skills, capacity) b. Number of clearly defined roles, responsibilities and prerogatives of project manager, assigned staff and other involved parties
Activities	**Capability Level**
1. Identify business and IT resource needs for the project and clearly map appropriate roles and responsibilities, with escalation and decision-making authorities agreed and understood.	2
2. Identify required skills and time requirements for all individuals involved in the project phases in relation to defined roles. Staff the roles based on available skills information (e.g., IT skills matrix).	
3. Utilize experienced project management and team leader resources with skills appropriate to the size, complexity and risk of the project.	
4. Consider and clearly define the roles and responsibilities of other involved parties, including finance, legal, procurement, HR, internal audit and compliance.	
5. Clearly define and agree on the responsibility for procurement and management of third-party products and services, and manage the relationships.	
6. Identify and authorize the execution of the work according to the project plan.	
7. Identify project plan gaps and provide feedback to the project manager to remediate.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.3 Direct and manage project work

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI11.09 Close a project or iteration. At the end of each project, release or iteration, require the project stakeholders to ascertain whether the project, release or iteration delivered the required results in terms of capabilities and contributed as expected to program benefits. Identify and communicate any outstanding activities required to achieve planned results of the project and/or benefits of the program. Identify and document lessons learned for future projects, releases, iterations and programs.	a. Level of stakeholder satisfaction expressed at project closure review b. Percent of outcomes with first-time acceptance

Activities	Capability Level
1. Obtain stakeholder acceptance of project deliverables and transfer ownership.	2
2. Define and apply key steps for project closure, including post-implementation reviews that assess whether a project attained desired results.	3
3. Plan and execute post-implementation reviews to determine whether projects delivered expected results. Improve the project management and system development process methodology.	
4. Identify, assign, communicate and track any uncompleted activities required to ensure the project delivered the required results in terms of capabilities and the results contributed as expected to the program benefits.	
5. Regularly, and upon completion of the project, collect lessons learned from the project participants. Review them and the key activities that led to delivered benefits and value. Analyze the data and make recommendations for improving the current project and the project management method for future projects.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 4.7 Close project or phase

B. Component: Organizational Structures

Key Management Practice	Chief Executive Officer	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Business Process Owners	Steering (Programs/Projects) Committee	Program Manager	Project Manager	Project Management Office	Head Development	Information Security Manager
BAI11.01 Maintain a standard approach for project management.	A		R				R	R			
BAI11.02 Start up and initiate a project.		R		R	R	A	R	R	R	R	
BAI11.03 Manage stakeholder engagement.			R			A		R			
BAI11.04 Develop and maintain the project plan.						A		R	R		
BAI11.05 Manage project quality.		R	R			A		R			R
BAI11.06 Manage project risk.			R			A		R			R
BAI11.07 Monitor and control projects.					R	A		R	R	R	
BAI11.08 Manage project resources and work packages.					R	A	R		R	R	
BAI11.09 Close a project or iteration.						A		R	R		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 3. The role of the project manager

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
BAI11.01 Maintain a standard approach for project management.	APO03.04	• Architecture governance requirements • Implementation phase descriptions	Updated project management approaches	Internal
	APO10.04	Identified vendor delivery risk		
	EDM02.03	Requirements for stage-gate reviews		
	EDM02.04	Actions to improve value delivery		
BAI11.02 Start up and initiate a project.			Project definitions	Internal
			Project scope statements	Internal
BAI11.03 Manage stakeholder engagement.			Results of stakeholder engagement effectiveness assessments	Internal
			Stakeholder engagement plan	Internal
BAI11.04 Develop and maintain the project plan.	BAI07.03	Approved acceptance test plan	Project reports and communications	Internal
			Project baseline	Internal
			Project plans	Internal
BAI11.05 Manage project quality.	APO11.01	Quality management plans	Project quality management plan	BAI02.04; BAI03.06; BAI07.01
	APO11.02	Customer requirements for quality management	Requirements for independent verification of project deliverables	BAI07.03
BAI11.06 Manage project risk.	APO12.02	Risk analysis results	Project risk register	Internal
	BAI02.03	• Requirements risk register • Risk mitigation actions	Project risk assessment results	Internal
	Outside COBIT	Enterprise risk management (ERM) framework	Project risk management plan	Internal
BAI11.07 Monitor and control projects.			Agreed changes to project	Internal
			Project progress reports	Internal
			Project performance criteria	Internal
BAI11.08 Manage project resources and work packages.			Project resource requirements	APO07.05; APO07.06
			Gaps in project planning	Internal
			Project roles and responsibilities	Internal

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI11.09 Close a project or iteration.	**From**	**Description**	**Description**	**To**
	BAI07.08	• Post-implementation review report • Remedial action plan	Post-implementation review results	APO02.04
			Stakeholder project acceptance confirmations	Internal
			Project lessons learned	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
PMBOK Guide Sixth Edition, 2017		Part 1: 4. Project integration management: Inputs and Outputs; Part 1: 6. Project schedule management: Inputs and Outputs; Part 1: 10. Project communications management: Inputs & Outputs; Part 1: 11. Project risk management: Inputs and Outputs		

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Portfolio, program and project support	Skills Framework for the Information Age V6, 2015	PROF
Project and portfolio management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.2. Project and Portfolio Management
Project management	Skills Framework for the Information Age V6, 2015	PRMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Program/project management policy	Guides management of risk related to programs and projects. Details management position and expectation regarding program and project management. Treats accountability, goals and objectives regarding performance, budget, risk analysis, reporting and mitigation of adverse events during program/project execution.	PMBOK guide Sixth edition, 2017	Part 1: 2.3.1 Processes, policies and procedures

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish an enterprisewide project management culture that ensures consistent and optimal implementation of project management across the enterprise, taking into account organizational structure and business environment. Ensure that all initiatives are translated into projects (or changes, where minor in scope); ensure that no ad hoc actions occur outside the scope of project management.		

G. Component: Services, Infrastructure and Applications
Project management tools

4.4 Deliver, Service and Support (DSS)

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS01 - Managed Operations	Focus Area: COBIT Core Model

Description

Coordinate and execute the activities and operational procedures required to deliver internal and outsourced I&T services. Include the execution of predefined standard operating procedures and the required monitoring activities.

Purpose

Deliver I&T operational product and service outcomes as planned.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality	AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

A. Component: Process

Management Practice	Example Metrics
DSS01.01 Perform operational procedures. Maintain and perform operational procedures and operational tasks reliably and consistently.	a. Number of incidents caused by operational problems b. Number of nonstandard operational procedures executed

Activities	Capability Level
1. Develop and maintain operational procedures and related activities to support all delivered services.	2
2. Maintain a schedule of operational activities and perform the activities.	
3. Verify that all data expected for processing are received and processed completely, accurately and in a timely manner. Deliver output in accordance with enterprise requirements. Support restart and reprocessing needs. Ensure that users are receiving the right outputs in a secure and timely manner.	3
4. Manage the performance and throughput of the scheduled activities.	4
5. Monitor incidents and problems dealing with operational procedures and take appropriate action to improve reliability of operational tasks performed.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	TP.SE Safeguard Operational Environment
HITRUST CSF version 9, September 2017	09.01 Document Operating Procedures
ISO/IEC 27002:2013/Cor.2:2015(E)	12.1 Operational procedures and responsibilities
ITIL V3, 2011	Service Operation, 4.1 Event Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.13 Physical and environmental protection (PE-13, PE-14, PE-15)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS01.02 Manage outsourced I&T services. Manage the operation of outsourced I&T services to maintain the protection of enterprise information and reliability of service delivery.	a. Number of specific/smart KPIs included in outsourcing contracts b. Frequency of failure by outsourcing partner to meet KPIs
Activities	**Capability Level**
1. Ensure that the enterprise's requirements for security of information processes adhere to contracts and SLAs with third parties hosting or providing services.	3
2. Ensure that the enterprise's operational business and IT processing requirements and priorities for service delivery adhere to contracts and SLAs with third parties hosting or providing services.	
3. Integrate critical internal IT management processes with those of outsourced service providers. This should cover, for example, performance and capacity planning, change management, configuration management, service request and incident management, problem management, security management, business continuity, and the monitoring of process performance and reporting.	
4. Plan for independent audit and assurance of the operational environments of outsourced providers to confirm that agreed requirements are being adequately addressed.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SC1.2 Outsourcing
ISO/IEC 20000-1:2011(E)	4.2 Governance of processes operated by other parties
Management Practice	**Example Metrics**
DSS01.03 Monitor I&T infrastructure. Monitor the I&T infrastructure and related events. Store sufficient chronological information in operations logs to reconstruct and review time sequences of operations and other activities surrounding or supporting operations.	a. Percent of critical operational event types covered by automatic detection systems b. Percent of infrastructure assets monitored based on service criticality and the relationship between configuration items and services that depend on them
Activities	**Capability Level**
1. Log events. Identify the level of information to be recorded, based on a consideration of risk and performance.	2
2. Identify and maintain a list of infrastructure assets that need to be monitored, based on service criticality and the relationship between configuration items and services that depend on them.	3
3. Define and implement rules that identify and record threshold breaches and event conditions. Find a balance between generating spurious minor events and significant events so event logs are not overloaded with unnecessary information.	
4. Produce event logs and retain them for an appropriate period to assist in future investigations.	
5. Ensure that incident tickets are created in a timely manner when monitoring identified deviations from defined thresholds.	
6. Establish procedures for monitoring event logs. Conduct regular reviews.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.10 Maintenance (MA-2, MA-3)
Management Practice	**Example Metrics**
DSS01.04 Manage the environment. Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	a. Number of people trained to respond to environmental alarm procedures b. Number of risk scenarios defined for environmental threats

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Identify natural and man-made disasters that might occur in the area where the IT facilities are located. Assess the potential effect on the IT facilities.	2
2. Identify how I&T equipment, including mobile and off-site equipment, is protected against environmental threats. Ensure that the policy limits or excludes eating, drinking and smoking in sensitive areas, and prohibits storage of stationery and other supplies that pose a fire hazard within computer rooms.	
3. Keep the IT sites and server rooms clean and in a safe condition at all times (i.e., no mess, no paper or cardboard boxes, no filled dustbins, no flammable chemicals or materials).	
4. Situate and construct IT facilities to minimize and mitigate susceptibility to environmental threats (e.g., theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals, explosives). Consider specific security zones and/or fireproof cells (e.g., locating production and development environments/servers away from each other).	3
5. Compare measures and contingency plans against insurance policy requirements and report results. Address points of noncompliance in a timely manner.	
6. Respond to environmental alarms and other notifications. Document and test procedures, which should include prioritization of alarms and contact with local emergency response authorities. Train personnel in these procedures.	
7. Regularly monitor and maintain devices that proactively detect environmental threats (e.g., fire, water, smoke, humidity).	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	2.1 System and system elements; 3.2 Categorization (Task 5, 6)
Management Practice	**Example Metrics**
DSS01.05 Manage facilities. Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.	a. Time since last test of uninterruptible power supply b. Number of people trained on health and safety guidelines
Activities	**Capability Level**
1. Examine the IT facilities' requirement for protection against power fluctuations and outages, in conjunction with other business continuity planning requirements. Procure suitable uninterruptible supply equipment (e.g., batteries, generators) to support business continuity planning.	2
2. Regularly test the uninterruptible power supply's mechanisms. Ensure that power can be switched to the supply without any significant effect on business operations.	
3. Ensure that the facilities housing the I&T systems have more than one source for dependent utilities (e.g., power, telecommunications, water, gas). Separate the physical entrance of each utility.	
4. Confirm that cabling external to the IT site is located underground or has suitable alternative protection. Determine that cabling within the IT site is contained within secured conduits, and access to wiring cabinets is restricted to authorized personnel. Properly protect cabling against damage caused by fire, smoke, water, interception and interference.	
5. Ensure that cabling and physical patching (data and phone) are structured and organized. Cabling and conduit structures should be documented (e.g., blueprint building plan and wiring diagrams).	
6. On regular basis, educate personnel on health and safety laws, regulations, and relevant guidelines. Educate personnel on fire and rescue drills to ensure knowledge and actions taken in case of fire or similar incidents.	
7. Ensure that IT sites and equipment are maintained according to the supplier's recommended service intervals and specifications. Ensure that maintenance is carried out only by authorized personnel.	3
8. Analyze the facilities housing's high-availability systems for redundancy and fail-over cabling requirements (external and internal).	
9. Ensure that IT sites and facilities are in ongoing compliance with relevant health and safety laws, regulations, guidelines, and vendor specifications.	
10. Record, monitor, manage and resolve facilities incidents in line with the I&T incident management process. Make available reports on facilities incidents for which disclosure is required by laws and regulations.	4
11. Analyze physical alterations to IT sites or premises to reassess the environmental risk (e.g., fire or water damage). Report results of this analysis to business continuity and facilities management.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures

Key Management Practice	Chief Operating Officer	Chief Information Officer	Chief Technology Officer	Head IT Operations	Information Security Manager	Privacy Officer
DSS01.01 Perform operational procedures.	R	A	R	R		
DSS01.02 Manage outsourced I&T services.		A	R	R	R	R
DSS01.03 Monitor I&T infrastructure.		R	A	R	R	
DSS01.04 Manage the environment.		R	A	R	R	
DSS01.05 Manage facilities.		R	A	R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

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

Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS01.01 Perform operational procedures.	BAI05.05	Operation and use plan	Backup log	Internal
			Operational schedule	Internal
DSS01.02 Manage outsourced I&T services.	APO09.03	• SLAs • OLAs	Independent assurance plans	MEA04.02
	BAI05.05	Operation and use plan		
DSS01.03 Monitor I&T infrastructure.	BAI03.11	Service definitions	Asset monitoring rules and event conditions	DSS02.01; DSS02.02
			Incident tickets	DSS02.02
			Event logs	Internal
DSS01.04 Manage the environment.			Environmental policies	APO01.09
			Insurance policy reports	MEA03.03
DSS01.05 Manage facilities.			Health and safety awareness	Internal
			Facilities assessment reports	MEA01.03

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.2 Categorization (Task 5, 6): Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Database administration	Skills Framework for the Information Age V6, 2015	DBAD
Facilities management	Skills Framework for the Information Age V6, 2015	DCMA
IT infrastructure	Skills Framework for the Information Age V6, 2015	ITOP
Methods and tools	Skills Framework for the Information Age V6, 2015	METL
Service delivery	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	C. Run—C.3. Service Delivery
Storage management	Skills Framework for the Information Age V6, 2015	STMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Service management policy	Provides direction and guidance to ensure effective management and implementation of all I&T services to meet business and customer requirements, within a framework of performance measurement. Covers management of risk related to I&T services. (The ITIL V3 framework offers detailed guidance on service management and optimization of risk related to services.)	(1) ISO/IEC 20000-1:2011(E); (2) ITIL V3, 2011	(1) 4.1.2 Service management policy; (2) Service Strategy, 3. Service strategy principles

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture of habitual excellence throughout the organization. Encourage employees to excel. Create an environment in which operational procedures deliver (more than) the necessary services while also allowing employees to question the status quo and try new ideas. Manage operational excellence through employee engagement and continuous improvement. Apply a customer-centric approach (for both internal and external customers).		

G. Component: Services, Infrastructure and Applications
• Cloud hosting services • Infrastructure monitoring tools • Service level monitoring tools

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS02 - Managed Service Requests and Incidents	Focus Area: COBIT Core Model

Description

Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.

Purpose

Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents. Assess the impact of changes and deal with service incidents. Resolve user requests and restore service in response to incidents.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality	AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

A. Component: Process

Management Practice	Example Metrics
DSS02.01 Define classification schemes for incidents and service requests. Define classification schemes and models for incidents and service requests.	a. Total number of service requests and incidents per priority level b. Total number of incidents escalated

Activities	Capability Level
1. Define incident and service request classification and prioritization schemes, and criteria for problem registration. Use this information to ensure consistent approaches for handling and informing users about problems and conducting trend analysis.	3
2. Define incident models for known errors to enable efficient and effective resolution.	
3. Define service request models according to service request type to enable self-help and efficient service for standard requests.	
4. Define incident escalation rules and procedures, especially for major incidents and security incidents.	
5. Define knowledge sources on incidents and requests and describe how to use them.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	IA.IP Implement Incident Investigation Processes
HITRUST CSF version 9, September 2017	11.01 Reporting Information Security Incidents and Weaknesses
ISF, The Standard of Good Practice for Information Security 2016	TM2 Security Incident Management
ISO/IEC 20000-1:2011(E)	8.1 Incident and service request management
ISO/IEC 27002:2013/Cor.2:2015(E)	16. Information security incident management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS02.02 Record, classify and prioritize requests and incidents. Identify, record and classify service requests and incidents and assign a priority according to business criticality and service agreements.	a. Number of types and categories defined for recording service requests and incidents b. Number of service requests and incidents that are not categorized
Activities	**Capability Level**
1. Log all service requests and incidents, recording all relevant information, so they can be handled effectively and a full historical record can be maintained.	2
2. To enable trend analysis, classify service requests and incidents by identifying type and category.	
3. Prioritize service requests and incidents based on the SLA service definition of business impact and urgency.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
DSS02.03 Verify, approve and fulfill service requests. Select the appropriate request procedures and verify that the service requests fulfill defined request criteria. Obtain approval, if required, and fulfill the requests.	a. Mean elapsed time for handling each type of service request b. Percent of service requests that fulfill defined request criteria
Activities	**Capability Level**
1. Verify entitlement for service requests using, where possible, a predefined process flow and standard changes.	2
2. Obtain financial and functional approval or sign-off, if required, or predefined approvals for agreed standard changes.	
3. Fulfill the requests by performing the selected request procedure. Where possible, use self-help automated menus and predefined request models for frequently requested items.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Operation, 4.3 Request Fulfilment
Management Practice	**Example Metrics**
DSS02.04 Investigate, diagnose and allocate incidents. Identify and record incident symptoms, determine possible causes, and allocate for resolution.	a. Number of identified and recorded incident symptoms b. Number of correctly determined symptom causes c. Number of duplicate problems in the reference log
Activities	**Capability Level**
1. Identify and describe relevant symptoms to establish the most probable causes of the incidents. Reference available knowledge resources (including known errors and problems) to identify possible incident resolutions (temporary workarounds and/or permanent solutions).	2
2. If a related problem or known error does not already exist and if the incident satisfies agreed criteria for problem registration, log a new problem.	
3. Assign incidents to specialist functions if deeper expertise is needed. Engage the appropriate level of management, where and if needed.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
DSS02.05 Resolve and recover from incidents. Document, apply and test the identified solutions or workarounds. Perform recovery actions to restore the I&T-related service.	a. Percent of incidents resolved within agreed SLA b. Percent of stakeholder satisfaction with resolution and recovery from incident
Activities	**Capability Level**
1. Select and apply the most appropriate incident resolutions (temporary workaround and/or permanent solution).	2
2. Record whether workarounds were used for incident resolution.	
3. Perform recovery actions, if required.	
4. Document incident resolution and assess if the resolution can be used as a future knowledge source.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Operation, 4.2 Incident Management
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	RC.RP Recovery Planning
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.9 Incident response (IR-4, IR-5, IR-6)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 201	CSC 19: Incident Response and Management
Management Practice	**Example Metrics**
DSS02.06 Close service requests and incidents. Verify satisfactory incident resolution and/or fulfilment of requests, and close.	a. Level of user satisfaction with service request fulfilment b. Percent of incidents resolved within an agreed/acceptable period of time

Activities	Capability Level
1. Verify with the affected users that the service request has been fulfilled satisfactorily or the incident has been resolved satisfactorily and within an agreed/acceptable period of time.	2
2. Close service requests and incidents.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	
Management Practice	**Example Metrics**
DSS02.07 Track status and produce reports. Regularly track, analyze and report incidents and fulfilment of requests. Examine trends to provide information for continual improvement.	a. Mean time between incidents for the I&T-enabled service b. Number and percent of incidents causing disruption to business-critical processes

Activities	Capability Level
1. Monitor and track incident escalations and resolutions and request handling procedures to progress toward resolution or completion.	2
2 Identify information stakeholders and their needs for data or reports. Identify reporting frequency and medium.	3
3. Produce and distribute timely reports or provide controlled access to online data.	4
4. Analyze incidents and service requests by category and type. Establish trends and identify patterns of recurring issues, SLA breaches or inefficiencies.	
5. Use the information as input to continual improvement planning.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	MI.IM Ensure Incident Mitigation; IR.IR Incident Reporting
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.9 Incident response (IR-7, IR-8)

B. Component: Organizational Structures						
Key Management Practice	Chief Technology Officer	Business Process Owners	Head Development	Head IT Operations	Service Manager	Information Security Manager
DSS02.01 Define classification schemes for incidents and service requests.	A		R	R	R	
DSS02.02 Record, classify and prioritize requests and incidents.	A			R	R	
DSS02.03 Verify, approve and fulfil service requests.	A	R	R	R	R	
DSS02.04 Investigate, diagnose and allocate incidents.	A	R		R	R	
DSS02.05 Resolve and recover from incidents.	A		R	R	R	R
DSS02.06 Close service requests and incidents.	A			R	R	R
DSS02.07 Track status and produce reports.	A			R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 27002:2013/Cor.2:2015(E)	16.1.1 Responsibilities and procedures

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS02.01 Define classification schemes for incidents and service requests.	APO09.03	SLAs	Criteria for problem registration	DSS03.01
	BAI10.02	Configuration repository	Rules for incident escalation	Internal
	BAI10.03	Updated repository with configuration items	Incident and service request classification schemes and models	Internal
	BAI10.04	Configuration status reports		
	DSS01.03	Asset monitoring rules and event conditions		
	DSS03.01	Problem classification scheme		
	DSS04.03	Incident response actions and communications		
DSS02.02 Record, classify and prioritize requests and incidents.	APO09.03	SLAs	Classified and prioritized incidents and service requests	APO08.03; APO09.04; APO13.03; DSS03.05
	BAI04.05	Emergency escalation procedure	Incident and service request log	Internal; MEA04.07
	DSS01.03	• Asset monitoring rules and event conditions • Incident tickets		
	DSS05.07	Security-related incident tickets		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS02.03 Verify, approve and fulfil service requests.	**From**	**Description**	**Description**	**To**
	APO12.06	Risk-related root causes	Approved service requests	BAI06.01
			Fulfilled service requests	Internal
DSS02.04 Investigate, diagnose and allocate incidents.	BAI07.07	Supplemental support plan	Problem log	DSS03.01
			Incident symptoms	Internal
DSS02.05 Resolve and recover from incidents.	APO12.06	Risk-related incident response plans	Incident resolutions	DSS03.03; DSS03.04; DSS03.05; MEA04.07
	DSS03.03	Known error records		
	DSS03.04	Communication of knowledge learned		
DSS02.06 Close service requests and incidents.	DSS03.04	Closed problem records	User confirmation of satisfactory fulfilment or resolution	APO08.03
			Closed service requests and incidents	APO08.03; APO09.04; DSS03.04
DSS02.07 Track status and produce reports.	APO09.03	OLAs	Incident status and trends report	APO08.03; APO09.04; APO11.04; APO12.01; MEA01.03
	DSS03.01	Problem status reports	Request fulfilment status and trends report	APO08.03; APO09.04; APO11.04; MEA01.03
	DSS03.02	Problem resolution reports		
	DSS03.05	Problem resolution monitoring reports		
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Application support	Skills Framework for the Information Age V6, 2015	ASUP
Customer service support	Skills Framework for the Information Age V6, 2015	CSMG
Incident management	Skills Framework for the Information Age V6, 2015	USUP
Network support	Skills Framework for the Information Age V6, 2015	NTAS
User support	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	C. Run—C.1. User Support

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Service request policy	States rationale and provides guidance for service and incident requests and their documentation.	ITIL V3, 2011	Service Operation, 3. Service operation principles

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Enable employees to identify incidents on a correct and timely basis and implement appropriate escalation paths. Encourage prevention. Respond to and resolve incidents immediately. Avoid a hero culture.		

G. Component: Services, Infrastructure and Applications
Incident tracking tools and system

Domain: Deliver, Service and Support Management Objective: DSS03 - Managed Problems	Focus Area: COBIT Core Model

Description

Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents. Provide recommendations for improvements.

Purpose

Increase availability, improve service levels, reduce costs, improve customer convenience and satisfaction by reducing the number of operational problems, and identify root causes as part of problem resolution.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG08 Optimization of internal business process functionality	AG05 Delivery of I&T services in line with business requirements
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

A. Component: Process

Management Practice	Example Metrics
DSS03.01 Identify and classify problems. Define and implement criteria and procedures to identify and report problems. Include problem classification, categorization and prioritization.	a. Percent of major incidents for which problems were logged b. Percent of incidents solved in accordance with agreed SLAs c. Percent of problems appropriately identified, including classification, categorization and prioritization

Activities	Capability Level
1. Identify problems through the correlation of incident reports, error logs and other problem identification resources.	2
2. Handle all problems formally with access to all relevant data. Include information from the IT change management system and IT configuration/asset and incident details.	
3. Define appropriate support groups to assist with problem identification, root cause analysis and solution determination to support problem management. Determine support groups based on predefined categories, such as hardware, network, software, applications and support software.	
4. Define priority levels through consultation with the business to ensure that problem identification and root cause analysis are handled in a timely manner according to the agreed SLAs. Base priority levels on business impact and urgency.	
5. Report the status of identified problems to the service desk so customers and IT management can be kept informed.	
6. Maintain a single problem management catalog to register and report problems identified. Use the catalog to establish audit trails of the problem management processes, including the status of each problem (i.e., open, reopen, in progress or closed).	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	8.2 Problem management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS03.02 Investigate and diagnose problems. Investigate and diagnose problems using relevant subject matter experts to assess and analyze root causes.	a. Number of identified problems classified as known errors b. Percent of problems investigated and diagnosed throughout their life cycle

Activities	Capability Level
1. Identify problems that may be known errors by comparing incident data with the database of known and suspected errors (e.g., those communicated by external vendors). Classify problems as known errors.	3
2. Associate the affected configuration items to the established/known error.	
3. Produce reports to communicate the progress in resolving problems and to monitor the continuing impact of problems not solved. Monitor the status of the problem-handling process throughout its life cycle, including input from IT change and configuration management.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
DSS03.03 Raise known errors. As soon as root causes of problems are identified, create known-error records, document appropriate workarounds and identify potential solutions.	a. Number of problems with satisfactory resolution that addressed root causes b. Percent of stakeholder satisfaction with identification of root causes, creation of known-error records and appropriate workarounds, and identification of potential solutions

Activities	Capability Level
1. As soon as the root causes of problems are identified, create known-error records and develop a suitable workaround.	2
2. Identify, evaluate, prioritize and process (via IT change management) solutions to known errors, based on a cost/benefit business case and business impact and urgency.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
DSS03.04 Resolve and close problems. Identify and initiate sustainable solutions addressing the root cause. Raise change requests via the established change management process, if required, to resolve errors. Ensure that the personnel affected are aware of the actions taken and the plans developed to prevent future incidents from occurring.	a. Decrease in number of recurring incidents caused by unresolved problems b. Percent of workarounds defined for open problems

Activities	Capability Level
1. Close problem records either after confirmation for successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.	2
2. Inform the service desk of the schedule for problem closure (e.g., the schedule for fixing the known errors, the possible workaround or the fact that the problem will remain until the change is implemented) and the consequences of the approach taken. Keep affected users and customers informed as appropriate.	
3. Throughout the resolution process, obtain regular reports from IT change management on progress in resolving problems and errors.	3
4. Monitor the continuing impact of problems and known errors on services.	4
5. Review and confirm the success of resolutions of major problems.	
6. Make sure the knowledge learned from the review is incorporated into a service review meeting with the business customer.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS03.05 Perform proactive problem management. Collect and analyze operational data (especially incident and change records) to identify emerging trends that may indicate problems. Log problem records to enable assessment.	a. Percent of problems logged as part of the proactive problem management activity b. Percent of key stakeholder satisfaction with the communication of problem information related to IT changes and incidents

Activities	Capability Level
1. Capture problem information related to I&T changes and incidents and communicate it to key stakeholders. Communicate via reports and periodic meetings among incident, problem, change and configuration management process owners to consider recent problems and potential corrective actions.	3
2. Ensure that process owners and managers from incident, problem, change and configuration management meet regularly to discuss known problems and future planned changes.	
3. Identify and initiate sustainable solutions (permanent fixes) addressing the root cause. Raise change requests via the established change management processes.	
4. To enable the enterprise to monitor the total costs of problems, capture change efforts resulting from problem management process activities (e.g., fixes to problems and known errors) and report on them.	4
5. Produce reports to monitor problem resolution against the business requirements and SLAs. Ensure the proper escalation of problems, such as escalating to a higher management level according to agreed criteria, contacting external vendors, or referring to the change advisory board to increase the priority of an urgent request for change (RFC) to implement a temporary workaround.	
6. To optimize the use of resources and reduce workarounds, track problem trends.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	MI.IC Ensure Incident Containment
ITIL V3, 2011	Service Operation, 4.4 Problem Management

B. Component: Organizational Structures							
Key Management Practice	**Executive Committee**	**Chief Information Officer**	**Chief Technology Officer**	**Head Development**	**Head IT Operations**	**Service Manager**	**Information Security Manager**
DSS03.01 Identify and classify problems.		R	A	R	R	R	
DSS03.02 Investigate and diagnose problems.			A		R	R	R
DSS03.03 Raise known errors.			A		R	R	R
DSS03.04 Resolve and close problems.			A		R	R	
DSS03.05 Perform proactive problem management.	R		A		R	R	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
DSS03.01 Identify and classify problems.	From	Description	Description	To
	APO12.06	Risk-related root causes	Problem classification scheme	DSS02.01
	DSS02.01	Criteria for problem registration	Problem status reports	DSS02.07
	DSS02.04	Problem log	Problem register	Internal
DSS03.02 Investigate and diagnose problems.	APO12.06	Risk-related root causes	Problem resolution reports	DSS02.07
			Root causes of problems	Internal; DSS03.05
DSS03.03 Raise known errors.	APO12.06	Risk-related root causes	Proposed solutions to known errors	BAI06.01
	DSS02.05	Incident resolutions	Known error records	DSS02.05
DSS03.04 Resolve and close problems.	DSS02.05	Incident resolutions	Communication of knowledge learned	APO08.04; DSS02.05
	DSS02.06	Closed service requests and incidents	Closed problem records	DSS02.06
DSS03.05 Perform proactive problem management.	APO12.06	Risk-related root causes	Identified sustainable solutions	BAI06.01
	DSS02.02	• Classified and prioritized incidents and service requests • Incident resolutions	Problem resolution monitoring reports	DSS02.07, MEA04.07
	DSS03.04	Root causes of problems		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Application support	Skills Framework for the Information Age V6, 2015	ASUP
Network support	Skills Framework for the Information Age V6, 2015	NTAS
Problem management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	C. Run—C.4. Problem Management
Problem management	Skills Framework for the Information Age V6, 2015	PBMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Problem resolution policy	Documents rationale and provides guidance for addressing problems that result from incidents and identifying validated workarounds.	ITIL V3, 2011	Service Operation, 3. Service operation principles

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Support a culture of proactive problem management (detection, action and prevention) with clearly defined roles and responsibilities. Ensure a transparent and open environment for reporting problems by providing independent reporting mechanisms and/or rewarding people who bring problems forward.		

G. Component: Services, Infrastructure and Applications
Problem tracking/resolution system

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS04 - Managed Continuity	Focus Area: COBIT Core Model

Description

Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise.

Purpose

Adapt rapidly, continue business operations and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG02 Managed business risk • EG06 Business service continuity and availability • EG08 Optimization of internal business process functionality	• AG05 Delivery of I&T services in line with business requirements • AG07 Security of information, processing infrastructure and applications, and privacy

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05	a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
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		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		

A. Component: Process	
Management Practice	**Example Metrics**
DSS04.01 Define the business continuity policy, objectives and scope. Define business continuity policy and scope, aligned with enterprise and stakeholder objectives, to improve business resilience.	a. Percent of business continuity objectives and scope reworked due to misidentified processes and activities b. Percent of key stakeholders participating, defining and agreeing on continuity policy and scope
Activities	**Capability Level**
1. Identify internal and outsourced business processes and service activities that are critical to the enterprise operations or necessary to meet legal and/or contractual obligations.	2
2. Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.	
3. Define and document the agreed minimum policy objectives and scope for business resilience.	
4. Identify essential supporting business processes and related I&T services.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	12.01 Information Security Aspects of Business Continuity Management
ISF, The Standard of Good Practice for Information Security 2016	BC1.1 Business Continuity Strategy; BC1.2 Business Continuity Programme
ISO/IEC 27002:2013/Cor.2:2015(E)	17. Information security aspects of business continuity management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-1)
Management Practice	**Example Metrics**
DSS04.02 Maintain business resilience. Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption.	a. Total downtime resulting from major incident or disruption b. Percent of key stakeholders involved in business impact analyses evaluating the impact over time of a disruption to critical business functions and the effect that a disruption would have on them
Activities	**Capability Level**
1. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.	2
2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.	
3. Establish the minimum time required to recover a business process and supporting I&T, based on an acceptable length of business interruption and maximum tolerable outage.	
4. Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.	
5. Assess the likelihood of threats that could cause loss of business continuity. Identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.	3
6. Analyze continuity requirements to identify possible strategic business and technical options.	
7. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.	
8. Obtain executive business approval for selected strategic options.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	BC1.3 Resilient Technical Environments
ITIL V3, 2011	Service Design, 4.6 IT Continuity Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-2)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS04.03 Develop and implement a business continuity response. Develop a business continuity plan (BCP) and disaster recovery plan (DRP) based on the strategy. Document all procedures necessary for the enterprise to continue critical activities in the event of an incident.	a. Number of critical business systems not covered by the plan b. Percent of key stakeholders involved in developing BCPs and DRPs

Activities	Capability Level
1. Define the incident response actions and communications to be taken in the event of disruption. Define related roles and responsibilities, including accountability for policy and implementation.	2
2. Ensure that key suppliers and outsource partners have effective continuity plans in place. Obtain audited evidence as required.	
3. Define the conditions and recovery procedures that would enable resumption of business processing. Include updating and reconciliation of information databases to preserve information integrity.	
4. Develop and maintain operational BCPs and DRPs that contain the procedures to be followed to enable continued operation of critical business processes and/or temporary processing arrangements. Include links to plans of outsourced service providers.	
5. Define and document the resources required to support the continuity and recovery procedures, considering people, facilities and IT infrastructure.	
6. Define and document the information backup requirements required to support the plans. Include plans and paper documents as well as data files. Consider the need for security and off-site storage.	
7. Determine required skills for individuals involved in executing the plan and procedures.	
8. Distribute the plans and supporting documentation securely to appropriately authorized interested parties. Make sure the plans and documentation are accessible under all disaster scenarios.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	BC1.4 Crisis Management; BC2.1 Business Continuity Planning
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-6, CP-9, CP-10)

Management Practice	Example Metrics
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). Test continuity on a regular basis to exercise plans against predetermined outcomes, uphold business resilience and allow innovative solutions to be developed.	a. Frequency of tests b. Number of exercises and tests that achieved recovery objectives

Activities	Capability Level
1. Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP and DRP in meeting business risk.	2
2. Define and agree on stakeholder exercises that are realistic and validate continuity procedures. Include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.	
3. Assign roles and responsibilities for performing continuity plan exercises and tests.	
4. Schedule exercises and test activities as defined in the continuity plans.	3
5. Conduct a post-exercise debriefing and analysis to consider the achievement.	4
6. Based on the results of the review, develop recommendations for improving the current continuity plans.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	PP.RS Develop and Maintain Response Plans; PP.RP Develop and Maintain Recovery Plans
ISF, The Standard of Good Practice for Information Security 2016	BC2.3 Business Continuity Testing
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 20: Penetration Tests and Red Team Exercises

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS04.05 Review, maintain and improve the continuity plans. Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plans in accordance with the change control process to ensure that continuity plans are kept up to date and continually reflect actual business requirements.	a. Percent of agreed improvements to the plan that have been reflected in the plan b. Percent of continuity plans and business impact assessments that are up to date

Activities	Capability Level
1. On a regular basis, review the continuity plans and capability against any assumptions made and current business operational and strategic objectives.	3
2. On a regular basis, review the continuity plans to consider the impact of new or major changes to enterprise organization, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.	
3. Consider whether a revised business impact assessment may be required, depending on the nature of the change.	
4. Recommend changes in policy, plans, procedures, infrastructure, and roles and responsibilities. Communicate them as appropriate for management approval and processing via the IT change management process.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
DSS04.06 Conduct continuity plan training. Provide all concerned internal and external parties with regular training sessions regarding procedures and their roles and responsibilities in case of disruption.	a. Percent of internal and external stakeholders who received training b. Percent of relevant internal and external parties whose skills and competencies are current

Activities	Capability Level
1. Roll out BCP and DRP awareness and training.	2
2. Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.	3
3. Develop competencies based on practical training, including participation in exercises and tests.	
4. Based on the exercise and test results, monitor skills and competencies.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-4)

Management Practice	Example Metrics
DSS04.07 Manage backup arrangements. Maintain availability of business-critical information.	a. Percent of backup media transferred and stored securely b. Percent of successful and timely restoration from backup or alternate media copies

Activities	Capability Level
1. Back up systems, applications, data and documentation according to a defined schedule. Consider frequency (monthly, weekly, daily, etc.), mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention), type of backup (e.g., full vs. incremental), and type of media. Consider also automated online backups, data types (e.g., voice, optical), creation of logs, critical end-user computing data (e.g., spreadsheets), physical and logical location of data sources, security and access rights, and encryption.	2
2. Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.	
3. Periodically test and refresh archived and backup data.	
4. Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.BP Apply Backup Processes
HITRUST CSF version 9, September 2017	09.05 Information Back-Up
ISF, The Standard of Good Practice for Information Security 2016	SY2.3 Backup
ISO/IEC 27002:2013/Cor.2:2015(E)	12.3 Backup
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-3)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 10: Data Recovery Capability
Management Practice	**Example Metrics**
DSS04.08 Conduct post-resumption review. Assess the adequacy of the business continuity plan (BCP) and disaster response plan (DRP) following successful resumption of business processes and services after a disruption.	a. Percent of issues identified and subsequently addressed in the plan b. Percent of issues identified and subsequently addressed in training materials

Activities	Capability Level
1. Assess adherence to the documented BCP and DRP.	4
2. Determine the effectiveness of the plans, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organizational structures and relationships.	
3. Identify weaknesses or omissions in the plans and capabilities and make recommendations for improvement. Obtain management approval for any changes to the plans and apply via the enterprise change control process.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures														
Key Management Practice	**Executive Committee**	**Chief Operating Officer**	**Chief Information Officer**	**Chief Technology Officer**	**Chief Information Security Officer**	**Business Process Owners**	**Data Management Function**	**Head Architect**	**Head Development**	**Head IT Operations**	**Service Manager**	**Information Security Manager**	**Business Continuity Manager**
DSS04.01 Define the business continuity policy, objectives and scope.	R	A	R		R	R				R	R		R
DSS04.02 Maintain business resilience.	R	A	R			R		R		R		R	R
DSS04.03 Develop and implement a business continuity response.			R	R		R				R		R	A
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).			R	R		R				R		R	A
DSS04.05 Review, maintain and improve the continuity plans.		A	R	R	R	R				R			R
DSS04.06 Conduct continuity plan training.			R	R		R			R	R		R	A
DSS04.07 Manage backup arrangements.				A			R			R		R	R
DSS04.08 Conduct post-resumption review.			R	R	R	R				R			A

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
DSS04.01 Define the business continuity policy, objectives and scope.	**From**	**Description**	**Description**	**To**
	APO09.03	SLAs	Policy and objectives for business continuity	APO01.02
			Assessments of current continuity capabilities and gaps	Internal
			Disruptive incident scenarios	Internal
DSS04.02 Maintain business resilience.	APO12.06	• Risk impact communication • Risk-related root causes	Approved strategic options	APO02.05
			BIAs	APO12.02
			Continuity requirements	Internal
DSS04.03 Develop and implement a business continuity response.	APO09.03	OLAs	Incident response actions and communications	DSS02.01
			BCP	Internal
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).			Test results and recommendations	Internal
			Test exercises	Internal
			Test objectives	Internal
DSS04.05 Review, maintain and improve the continuity plans.			Recommended changes to plans	Internal
			Results of reviews of plans	Internal
DSS04.06 Conduct continuity plan training.	HR	List of personnel requiring training	Monitoring results of skills and competencies	APO07.03
			Training requirements	APO07.03
DSS04.07 Manage backup arrangements.	APO14.10	• Backup plan • Backup test plan	Test results of backup data	Internal
			Backup data	Internal; APO14.08
DSS04.08 Conduct post-resumption review.			Approved changes to the plans	BAI06.01
			Post-resumption review report	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Continuity management	Skills Framework for the Information Age V6, 2015	COPL

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Business continuity policy	Outlines management's commitment to the business impact assessment (BIA), business contingency plan (including trusted recovery), recovery requirements for critical systems, defined thresholds and triggers for contingencies, escalation plan, data recovery plan, training and testing.		
Crisis management policy	Sets guidelines and sequence of crisis response in key areas of risk. Along with I&T security, network management, and data security and privacy, crisis management is one of the operational-level policies that should be considered for complete I&T risk management.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Embed the need for business resilience in the enterprise culture. Regularly and frequently update employees about core values, desired behaviors and strategic objectives to maintain the enterprise's composure and image in every situation. Regularly test business continuity procedures and disaster recovery.		

G. Component: Services, Infrastructure and Applications
• External hosting services • Incident monitoring tools • Remote storage facility services

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS05 - Managed Security Services	Focus Area: COBIT Core Model

Description

Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges. Perform security monitoring.

Purpose

Minimize the business impact of operational information security vulnerabilities and incidents.

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	• AG02 Managed I&T-related risk • 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	AG02 a. Frequency of updating risk profile b. Percent of enterprise risk assessments including I&T-related risk c. Number of significant I&T-related incidents that were not identified in a risk assessment
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	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

A. Component: Process

Management Practice	Example Metrics
DSS05.01 Protect against malicious software. Implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e.g., ransomware, malware, viruses, worms, spyware, spam).	a. Number of successful malicious software attacks b. Percent of employees failing tests on malicious attacks (e.g., test of phishing email)

Activities	Capability Level
1. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).	2
2. Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails).	
3. Communicate malicious software awareness and enforce prevention procedures and responsibilities. Conduct periodic training about malware in email and Internet usage. Train users to not open, but report, suspicious emails and to not install shared or unapproved software.	3
4. Distribute all protection software centrally (version and patch-level) using centralized configuration and IT change management.	
5. Regularly review and evaluate information on new potential threats (e.g., reviewing vendors' products and services security advisories).	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	DP.DC Detect Malicious Code; RI.VT Vulnerability and Threat Identification
HITRUST CSF version 9, September 2017	09.04 Protection Against Malicious & Mobile Code
SF, The Standard of Good Practice for Information Security 2016	TS1 Security Solutions
SO/IEC 27002:2013/Cor.2:2015(E)	12.2 Protection against malware
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 4: Continuous Vulnerability Assessment and Remediation; CSC 8: Malware Defenses

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS05.02 Manage network and connectivity security. Use security measures and related management procedures to protect information over all methods of connectivity.	a. Number of firewall breaches b. Number of vulnerabilities discovered c. Percent of time network and systems not available due to security incident

Activities	Capability Level
1. Allow only authorized devices to have access to corporate information and the enterprise network. Configure these devices to force password entry.	2
2. Implement network filtering mechanisms, such as firewalls and intrusion detection software. Enforce appropriate policies to control inbound and outbound traffic.	
3. Apply approved security protocols to network connectivity.	
4. Configure network equipment in a secure manner.	
5. Encrypt information in transit according to its classification.	3
6. Based on risk assessments and business requirements, establish and maintain a policy for security of connectivity.	
7. Establish trusted mechanisms to support the secure transmission and receipt of information.	
8. Carry out periodic penetration testing to determine adequacy of network protection.	4
9. Carry out periodic testing of system security to determine adequacy of system protection.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	AC.MI Manage Network Integrity & Segregation; CM.MN Monitor Networks; AC.CP Manage Communication Protections
HITRUST CSF version 9, September 2017	01.04 Network Access Control
ISF, The Standard of Good Practice for Information Security 2016	PA2.3 Mobile Device Connectivity; NC1.1 Network Device Configuration
ISO/IEC 27002:2013/Cor.2:2015(E)	13.1 Network security management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.20 System and information integrity (SI-8)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 9: Limitation and Control of Network Ports, Protocols, and Services; CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Management Practice	Example Metrics
DSS05.03 Manage endpoint security. Ensure that endpoints (e.g., laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements for the information processed, stored or transmitted.	a. Number of incidents involving endpoint devices b. Number of unauthorized devices detected on the network or in the end-user environment c. Percent of individuals receiving awareness training relating to use of endpoint devices

Activities	Capability Level
1. Configure operating systems in a secure manner.	2
2. Implement device lockdown mechanisms.	
3. Manage remote access and control (e.g., mobile devices, teleworking).	
4. Manage network configuration in a secure manner.	
5. Implement network traffic filtering on endpoint devices.	
6. Protect system integrity.	
7. Provide physical protection of endpoint devices.	
8. Dispose of endpoint devices securely.	
9. Manage malicious access through email and web browsers. For example, block certain websites and deactivate click-through on links for smartphones.	
10. Encrypt information in storage according to its classification.	3

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.MM Apply Mobile Device Management; TP.MP Apply Media Protection; DP.DP Detect Mobile Code and Browser Protection
ISF, The Standard of Good Practice for Information Security 2016	PM1.3 Remote Working; PA2.1 Mobile Device Configuration; PA2.4 Employee-owned Devices; PA2.5 Portable Storage Devices; NC1.6 Remote Maintenance
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.4 Assessment, authorization and monitoring (CA-8, CA-9); 3.19 System and communications protection (SC-10)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers; CSC 7: Email and Web Browser Protections
Management Practice	**Example Metrics**
DSS05.04 Manage user identity and logical access. Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes.	a. Average time between change and update of accounts b. Number of accounts (vs. number of authorized users/staff) c. Number of incidents relating to unauthorized access to information
Activities	**Capability Level**
1. Maintain user access rights in accordance with business function, process requirements and security policies. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.	2
2. Administer all changes to access rights (creation, modifications and deletions) in a timely manner based only on approved and documented transactions authorized by designated management individuals.	3
3. Segregate, reduce to the minimum number necessary and actively manage privileged user accounts. Ensure monitoring on all activity on these accounts.	
4. Uniquely identify all information processing activities by functional roles. Coordinate with business units to ensure that all roles are consistently defined, including roles that are defined by the business itself within business process applications.	
5. Authenticate all access to information assets based on the individual's role or business rules. Coordinate with business units that manage authentication within applications used in business processes to ensure that authentication controls have been properly administered.	
6. Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable.	
7. Maintain an audit trail of access to information depending upon its sensitivity and regulatory requirements.	4
8. Perform regular management review of all accounts and related privileges.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	10.03 Cryptographic Controls
ISF, The Standard of Good Practice for Information Security 2016	PM1.1 Employment Life Cycle; SA1 Access Management
ISO/IEC 27002:2013/Cor.2:2015(E)	7.3 Termination and change of employment; 9. Access control
ITIL V3, 2011	Service Operation, 4.5 Access Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.1 Access control (AC-11, AC-12); 3.11 Media protection (MP-2, MP-4, MP-7); 3.13 Physical and environmental protection (PE-2, PE-3, PE-6)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software; CSC 5: Controlled Use of Administrative Privileges; CSC 16: Account Monitoring and Control

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS05.05 Manage physical access to I&T assets. Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	a. Average rating for physical security assessments b. Number of physical information security-related incidents

Activities	Capability Level
1. Log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site.	2
2. Ensure all personnel display properly approved identification at all times.	
3. Require visitors to be escorted at all times while on-site.	
4. Restrict and monitor access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls and security devices on interior and exterior doors.	
5. Manage requests to allow appropriately authorized access to the computing facilities.	3
6. Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.	
7. Conduct regular physical information security awareness training.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	AC.MA Manage Access; ID.DI Determine Impacts
HITRUST CSF version 9, September 2017	01.01 Business Requirement for Access Control; 01.02 Authorized Access to Information Systems; 02.0 Human Resources Security
ISF, The Standard of Good Practice for Information Security 2016	NC1.2 Physical Network Management
ISO/IEC 27002:2013/Cor.2:2015(E)	11. Physical and environmental security

Management Practice	Example Metrics
DSS05.06 Manage sensitive documents and output devices. Establish appropriate physical safeguards, accounting practices and inventory management regarding sensitive I&T assets, such as special forms, negotiable instruments, special-purpose printers or security tokens.	a. Number of stolen output devices b. Percent of sensitive documents and output devices identified in inventory

Activities	Capability Level
1. Establish procedures to govern the receipt, use, removal and disposal of sensitive documents and output devices into, within, and outside of the enterprise.	2
2. Ensure cryptographic controls are in place to protect sensitive electronically stored information.	
3. Assign access privileges to sensitive documents and output devices based on the least-privilege principle, balancing risk and business requirements.	3
4. Establish an inventory of sensitive documents and output devices, and conduct regular reconciliations.	
5. Establish appropriate physical safeguards over sensitive documents.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	CM.Ph Monitor Physical
HITRUST CSF version 9, September 2017	01.06 Application & Information Access Control; 01.07 Mobile Computing & Teleworking; 08.0 Physical & Environmental Security; 10.03 Cryptographic Controls; 10.04 Security of System Files
ISF, The Standard of Good Practice for Information Security 2016	IR2.3 Business Impact Assessment - Confidentiality Requirements; IR2.4 Business Impact Assessment - Integrity Requirements; IR2.5 Business Impact Assessment - Availability Requirements; IM2.2 Sensitive Physical Information; PA2.2 Enterprise Mobility Man
ISO/IEC 27002:2013/Cor.2:2015(E)	10. Cryptography
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.1 Access control (AC-2, AC-3, AC-4, AC-5, AC-6, AC-13, AC-24); 3.7 Identification and authentication (IA-2, IA-10, IA-11)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 15: Wireless Access Control
Management Practice	**Example Metrics**
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events. Using a portfolio of tools and technologies (e.g., intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	a. Number of vulnerability tests carried out on perimeter devices b. Number of vulnerabilities discovered during testing c. Time taken to remediate any vulnerabilities d. Percent of tickets created in a timely manner when monitoring systems identify potential security incidents

Activities	Capability Level
1. Continually use a portfolio of supported technologies, services and assets (e.g., vulnerability scanners, fuzzers and sniffers, protocol analyzers) to identify information security vulnerabilities.	2
2. Define and communicate risk scenarios, so they can be easily recognized, and the likelihood and impact understood.	
3. Regularly review the event logs for potential incidents.	
4. Ensure that security--related incident tickets are created in a timely manner when monitoring identifies potential incidents.	
5. Log security-related events and retain records for appropriate period.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	IR2.6 Threat Profiling
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.7 Identification and authentication (IA-3); 3.11 Media protection (MP-1); 3.13 Physical and environmental protection (PE-5); 3.19 System and communications protection (SC-15)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	Maintenance, Monitoring, and Analysis of Audit Logs

B. Component: Organizational Structures

Key Management Practice	Chief Information Officer	Chief Information Security Officer	Business Process Owners	Head Human Resources	Head Development	Head IT Operations	Information Security Manager	Privacy Officer
DSS05.01 Protect against malicious software.		A	R	R	R	R	R	
DSS05.02 Manage network and connectivity security.		A			R	R	R	
DSS05.03 Manage endpoint security.		A			R	R	R	
DSS05.04 Manage user identity and logical access.		A	R			R	R	R
DSS05.05 Manage physical access to I&T assets.		A				R	R	R
DSS05.06 Manage sensitive documents and output devices.	A					R		R
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.		A				R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

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

Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS05.01 Protect against malicious software.			Malicious software prevention policy	APO01.02
			Evaluations of potential threats	APO12.02; APO12.03
DSS05.02 Manage network and connectivity security.	APO01.07	Data classification guidelines	Connectivity security policy	APO01.02
	APO09.03	SLAs	Results of penetration tests	MEA04.07
DSS05.03 Manage endpoint security.	APO03.02	Information architecture model	Security policies for endpoint devices	APO01.02
	APO09.03	• SLAs • OLAs		
	BAI09.01	Results of physical inventory checks		
	DSS06.06	Reports of violations		
DSS05.04 Manage user identity and logical access.	APO01.05	Definition of I&T-related roles and responsibilities	Results of reviews of user accounts and privileges	Internal
	APO03.02	Information architecture model	Approved user access rights	Internal

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS05.05 Manage physical access to I&T assets.	**From**	**Description**	**Description**	**To**
			Access logs	DSS06.03, MEA04.07
			Approved access requests	Internal
DSS05.06 Manage sensitive documents and output devices.	APO03.02	Information architecture model	Access privileges	Internal
			Inventory of sensitive documents and devices	Internal
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.			Security incident tickets	DSS02.02
			Security incident characteristics	Internal
			Security event logs	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this component				

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 management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage— E.8. Information Security Management
Penetration testing	Skills Framework for the Information Age V6, 2015	PENT
Security administration	Skills Framework for the Information Age V6, 2015	SCAD

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Information security policy	Sets guidelines to protect corporate information and associated systems and infrastructure.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture of awareness regarding user responsibility to maintain security and privacy practices.	1) HITRUST CSF version 9, September 2017; (2) ISF, The Standard of Good Practice for Information Security 2016	(1) 01.03 User Responsibilities; (2) PM2.1 Security Awareness Program

G. Component: Services, Infrastructure and Applications
• Directory services • Email filtering systems • Identity and access management system • Security awareness services • Security information and event management (SIEM) tools • Security operations center (SOC) services • Third-party security assessment services • URL filtering systems

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS06 - Managed Business Process Controls	Focus Area: COBIT Core Model

Description

Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements. Manage and operate adequate input, throughput and output controls (application controls) to ensure that information and information processing satisfy these requirements.

Purpose

Maintain information integrity and the security of information assets handled within business processes in the enterprise or its outsourced operation.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG05 Customer-oriented service culture • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	AG08 Enabling and supporting business processes by integrating applications and technology

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG08	a. Time to execute business services or processes b. Number of I&T-enabled business programs delayed or incurring additional cost due to technology-integration issues c. Number of business process changes that need to be delayed or reworked because of technology-integration issues d. Number of applications or critical infrastructures operating in silos and not integrated
EG05	a. Number of customer service disruptions b. Percent of business stakeholders satisfied that customer service delivery meets agreed levels c. Number of customer complaints d. Trend of customer satisfaction survey results		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		
EG12	a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates		

A. Component: Process

Management Practice	Example Metrics
DSS06.01 Align control activities embedded in business processes with enterprise objectives. Continually assess and monitor the execution of business process activities and related controls (based on enterprise risk), to ensure that processing controls align with business needs.	a. Percent of completed inventory of critical processes and key controls b. Percent of processing controls aligned with business needs

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Identify and document the necessary control activities for key business processes to satisfy control requirements for strategic, operational, reporting and compliance objectives.	2
2. Prioritize control activities based on the inherent risk to the business. Identify key controls.	
3. Ensure ownership of key control activities.	
4. Implement automated controls.	3
5. Continually monitor control activities on an end-to-end basis to identify opportunities for improvement.	4
6. Continually improve the design and operation of business process controls.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 10, 11)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 14: Controlled Access Based on the Need to Know
Management Practice	**Example Metrics**
DSS06.02 Control the processing of information. Operate the execution of the business process activities and related controls, based on enterprise risk. Ensure that information processing is valid, complete, accurate, timely and secure (i.e., reflects legitimate and authorized business use).	a. Number of incidents and audit report findings indicating failure of key controls b. Percent of coverage of key controls within test plans
Activities	**Capability Level**
1. Authenticate the originator of transactions and verify that the individual has the authority to originate the transaction.	2
2. Ensure adequate segregation of duties regarding the origination and approval of transactions.	
3. Verify that transactions are accurate, complete and valid. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness, duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmations. Validate input data and edit or, where applicable, send back for correction as close to the point of origination as possible.	3
4. Without compromising original transaction authorization levels, correct and resubmit data that were erroneously input. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.	
5. Maintain the integrity and validity of data throughout the processing cycle. Ensure that detection of erroneous transactions does not disrupt processing of valid transactions.	
6. Handle output in an authorized manner, deliver it to the appropriate recipient and protect the information during transmission. Verify the accuracy and completeness of the output.	
7. Maintain the integrity of data during unexpected interruptions in business processing. Confirm data integrity after processing failures.	
8. Before passing transaction data between internal applications and business/operational functions (inside or outside the enterprise), check for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	13.01 Openness and Transparency; 13.02 Individual Choice and Participation
ISF, The Standard of Good Practice for Information Security 2016	BA1.4 Information Validation

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority. Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	a. Number of incidents and audit findings due to access or separation-of-duties violations b. Percent of business process roles with assigned access rights and levels of authority c. Percent of business process roles with clear separation of duties

Activities	Capability Level
1. Allocate roles and responsibilities based on approved job descriptions and business process activities.	2
2. Allocate levels of authority for approval of transactions, transaction limits and any other decisions relating to the business process, based on approved job roles.	
3. Allocate roles for sensitive activities so there is a clear segregation of duties.	
4. Allocate access rights and privileges based on the minimum that is required to perform job activities, based on pre-defined job roles. Remove or revise access rights immediately if the job role changes or a staff member leaves the business process area. Periodically review to ensure that the access is appropriate for the current threats, risk, technology and business need.	3
5. On a regular basis, provide awareness and training regarding roles and responsibilities so that everyone understands their responsibilities; the importance of controls; and the security, integrity, confidentiality and privacy of company information in all its forms.	
6. Ensure administrative privileges are sufficiently and effectively secured, tracked and controlled to prevent misuse.	
7. Periodically review access control definitions, logs and exception reports. Ensure that all access privileges are valid and aligned with current staff members and their allocated roles.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
HITRUST CSF version 9, September 2017	13.04 Collection, Use and Disclosure
ISO/IEC 27002:2013/Cor.2:2015(E)	7. Human resource security
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 5: Controlled Use of Administrative Privileges

Management Practice	Example Metrics
DSS06.04 Manage errors and exceptions. Manage business process exceptions and errors and facilitate remediation, executing defined corrective actions and escalating as necessary. This treatment of exceptions and errors provides assurance of the accuracy and integrity of the business information process.	a. Frequency of processing inefficiencies due to incomplete data entry b. Number of errors detected in a timely manner c. Number of data processing errors that were efficiently remediated

Activities	Capability Level
1. Review errors, exceptions and deviations.	2
2. Follow up, correct, approve and resubmit source documents and transactions.	
3. Maintain evidence of remedial actions.	
4. Define and maintain procedures to assign ownership for errors and exceptions, correct errors, override errors and handle out-of-balance conditions.	3
5. Report relevant business information process errors in a timely manner to perform root cause and trending analysis.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS06.05 Ensure traceability and accountability for information events. Ensure that business information can be traced to an originating business event and associated with accountable parties. This discoverability provides assurance that business information is reliable and has been processed in accordance with defined objectives.	a. Number of incidents in which transaction history cannot be recovered b. Percent of completeness of traceable transaction log
Activities	**Capability Level**
1. Capture source information, supporting evidence and the record of transactions.	2
2. Define retention requirements, based on business requirements, to meet operational, financial reporting and compliance needs.	3
3. Dispose of source information, supporting evidence and the record of transactions in accordance with the retention policy.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
DSS06.06 Secure information assets. Secure information assets accessible by the business through approved methods, including information in electronic form (e.g., portable media devices, user applications and storage devices, or other methods that create new assets in any form), information in physical form (e.g., source documents or output reports) and information during transit. This benefits the business by providing end-to-end safeguarding of information.	a. Cases of sensitive transaction data delivered to wrong recipient b. Frequency of compromised integrity of critical data
Activities	**Capability Level**
1. Restrict use, distribution and physical access of information according to its classification.	2
2. Provide acceptable use awareness and training.	
3. Apply data classification and acceptable use and security policies and procedures to protect information assets under the control of the business.	3
4. Identify and implement processes, tools and techniques to reasonably verify compliance.	
5. Report to business and other stakeholders on violations and deviations.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	AC.MP Manage Access Permissions
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 18: Application Software Security

B. Component: Organizational Structures										
Key Management Practice	Executive Committee	Chief Information Officer	I&T Governance Board	Chief Information Security Officer	Business Process Owners	Data Management Function	Service Manager	Information Security Manager	Legal Counsel
DSS06.01 Align control activities embedded in business processes with enterprise objectives.	R		A		R				
DSS06.02 Control the processing of information.		R	A	R	R	R			R
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.		R	A	R	R			R	
DSS06.04 Manage errors and exceptions.		R		R	A		R		
DSS06.05 Ensure traceability and accountability for information events.		R		R	A				
DSS06.06 Secure information assets.		R		R	A				

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
DSS06.01 Align control activities embedded in business processes with enterprise objectives.	APO01.07	• Data classification guidelines • Data integrity procedures	Root cause analyses and recommendations	BAI06.01; MEA02.04; MEA04.04; MEA04.06; MEA04.07
			Results of processing effectiveness reviews	MEA02.04
DSS06.02 Control the processing of information.	BAI05.05	Operation and use plan	Processing control reports	Internal
	BAI07.02	Migration plan		
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.	APO11.01	Quality management system (QMS) roles, responsibilities and decision rights	Allocated levels of authority	APO01.05
	APO13.01	Information security management system (ISMS) scope statement	Allocated roles and responsibilities	APO01.05
	DSS05.05	Access logs	Allocated access rights	APO07.04
	EDM04.02	Assigned responsibilities for resource management		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS06.04 Manage errors and exceptions.	**From**	**Description**	**Description**	**To**
			Error reports and root cause analysis	Internal
			Evidence of error correction and remediation	MEA02.04
DSS06.05 Ensure traceability and accountability for information events.			Record of transactions	Internal
			Retention requirements	Internal; APO14.09
DSS06.06 Secure information assets.			Reports of violations	DSS05.03

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 10, 11): 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
Security administration	Skills Framework for the Information Age V6, 2015	SCAD

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Business controls guidance	Defines business process controls to ensure proper control and reduce risk of fraud and errors. Identifies manual controls to protect documents (e.g., source, input, processing and output documents); identifies supervisory controls to review the flow of documents and ensure correct processing. Includes I&T general controls (e.g., physical security, access and authentication, and change management) and application controls (e.g., edit checking, system configuration and security settings).		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture that embraces the need for sound controls in business processes, building them into applications in development or requiring them in applications bought or accessed as a service. Encourage all employees to have a controls consciousness to protect all assets of the organization (e.g., paper records and facilities).		

G. Component: Services, Infrastructure and Applications
• Automated application controls • Event log auditing tools

4.5 Monitor, Evaluate and Assess (MEA)

Page intentionally left blank

Domain: Monitor, Evaluate and Assess Management Objective: MEA01 — Managed Performance and Conformance Monitoring	Focus Area: COBIT Core Model

Description

Collect, validate and evaluate enterprise and alignment goals and metrics. Monitor that processes and practices are performing against agreed performance and conformance goals and metrics. Provide reporting that is systematic and timely.

Purpose

Provide transparency of performance and conformance and drive achievement of goals.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG01 Portfolio of competitive products and services • EG04 Quality of financial information • EG07 Quality of management information • EG08 Optimization of internal business process functionality	• AG05 Delivery of I&T services in line with business requirements • AG10 Quality of I&T management information

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05	a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG04	a. Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information b. Cost of noncompliance with finance-related regulations	AG10	a. Level of user satisfaction with quality, timeliness and availability of I&T-related management information, taking into account available resources b. Ratio and extent of erroneous business decisions in which erroneous or unavailable I&T-related information was a key factor c. Percentage of information meeting quality criteria
EG07	a. Degree of board and executive management satisfaction with decision-making information b. Number of incidents caused by incorrect business decisions based on inaccurate information c. Time to provide information supporting effective business decisions d. Timeliness of management information		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		

A. Component: Process

Management Practice	Example Metrics
MEA01.01 Establish a monitoring approach. Engage with stakeholders to establish and maintain a monitoring approach to define the objectives, scope and method for measuring business solution and service delivery and contribution to enterprise objectives. Integrate this approach with the corporate performance management system.	a. Percent of processes with defined goals and metrics b. Percent of integration of monitoring approach within corporate performance management system

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Identify stakeholders (e.g., management, process owners and users).	2
2. Engage with stakeholders and communicate the enterprise requirements and objectives for monitoring, aggregating and reporting, using common definitions (e.g., business glossary, metadata and taxonomy), baselining and benchmarking.	
3. Align and continually maintain the monitoring and evaluation approach with the enterprise approach and the tools to be used for data gathering and enterprise reporting (e.g., business intelligence applications).	
4. Agree on the types of goals and metrics (e.g., conformance, performance, value, risk), taxonomy (classification and relationships between goals and metrics) and data (evidence) retention.	
5. Request, prioritize and allocate resources for monitoring, consider appropriateness, efficiency, effectiveness and confidentiality.	
6. Periodically validate the approach used and identify new or changed stakeholders, requirements and resources.	3
7. Agree on a life cycle management and change control process for monitoring and reporting. Include improvement opportunities for reporting, metrics, approach, baselining and benchmarking.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes - Measurement and Analysis
SF, The Standard of Good Practice for Information Security 2016	SI2 Security Performance
ISO/IEC 27001:2013/Cor.2:2015(E)	9.1 Monitoring, measurement, analysis and evaluation
ISO/IEC 27004:2016(E)	6. Characteristics; 7. Types of measures; 8. Processes
ISO/IEC 38500:2015(E)	5.5 Principle 4: Performance; 5.6 Principle 5: Conformance
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 13); 3.3 Selection (Task 2); 3.7 Monitoring (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.4 Assessment, authorization and monitoring (CA-2, CA-7); 3.20 System and information integrity (SI-4)

Management Practice	Example Metrics
MEA01.02 Set performance and conformance targets. Work with stakeholders to define, periodically review, update and approve performance and conformance targets within the performance measurement system.	a. Percent of goals and metrics approved by stakeholders b. Percent of processes with effectiveness of goals and metrics reviewed and improved

Activities	Capability Level
1. Define the goals and metrics. Periodically review them with stakeholders to identify any significant missing items and define reasonableness of targets and tolerances.	2
2. Evaluate whether the goals and metrics are adequate, that is, specific, measurable, achievable, relevant and time-bound (SMART).	
3. Communicate proposed changes to performance and conformance targets and tolerances (relating to metrics) with key due diligence stakeholders (e.g., legal, audit, HR, ethics, compliance, finance).	
4. Publish changed targets and tolerances to users of this information.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Management
National Institute of Standards and Technology Special Publication 800-53, Revisionv5 (Draft), August 2017	3.4 Assessment, authorization and monitoring (CA-5)

Management Practice	Example Metrics
MEA01.03 Collect and process performance and conformance data. Collect and process timely and accurate data aligned with enterprise approaches.	a. Percent of critical processes monitored b. Percent of controls environment that is monitored, benchmarked and improved to meet organizational objectives

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Collect data from defined processes (automated, where possible).	2
2. Assess efficiency (effort in relation to insight provided) and appropriateness (usefulness and meaning) of collected data and validate the data's integrity (accuracy and completeness).	
3. Aggregate data to support measurement of agreed metrics.	
4. Align aggregated data to the enterprise reporting approach and objectives.	3
5. Use suitable tools and systems for the processing and analysis of data.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.20 System and information integrity (SI-2)
Management Practice	**Example Metrics**
MEA01.04 Analyze and report performance. Periodically review and report performance against targets. Use a method that provides a succinct all-around view of I&T performance and fits within the enterprise monitoring system.	a. Percent of goals and metrics aligned to enterprise monitoring system b. Percent of performance reports delivered as scheduled c. Percent of processes with assured output meeting targets within tolerances
Activities	**Capability Level**
1. Design process performance reports that are concise, easy to understand, and tailored to various management needs and audiences. Facilitate effective, timely decision making (e.g., scorecards, traffic light reports). Ensure that the cause and effect between goals and metrics are communicated in an understandable manner.	3
2. Distribute reports to the relevant stakeholders.	
3. Analyze the cause of deviations against targets, initiate remedial actions, assign responsibilities for remediation, and follow up. At appropriate times, review all deviations and search for root causes, where necessary. Document the issues for further guidance if the problem recurs. Document results.	4
4. Where feasible, integrate performance and compliance into individual staff members' performance objectives and link achievement of performance targets to the organizational reward compensation system.	
5. Compare the performance values to internal targets and benchmarks and, where possible, to external benchmarks (industry and key competitors).	
6. Analyze trends in performance and compliance and take appropriate action.	
7. Recommend changes to the goals and metrics, where appropriate.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Measurement and Analysis
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.3 Audit and accountability (AU-6)
Management Practice	**Example Metrics**
MEA01.05 Ensure the implementation of corrective actions. Assist stakeholders in identifying, initiating and tracking corrective actions to address anomalies.	a. Number of recurring anomalies b. Number of corrective actions implemented
Activities	**Capability Level**
1. Review management responses, options and recommendations to address issues and major deviations.	2
2. Ensure that the assignment of responsibility for corrective action is maintained.	
3. Track the results of actions committed.	
4. Report the results to the stakeholders.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Continual Service Improvement, 4.1 The 7-Step Improvement Process
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.7 Monitoring (Task 3)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.3 Audit and accountability (AU-5)

B. Component: Organizational Structures												
Key Management Practice	Executive Committee	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Chief Information Officer	I&T Governance Board	Business Process Owners	Relationship Manager	Head Development	Head IT Operations	Service Manager
MEA01.01 Establish a monitoring approach.	R	A	R	R	R	R					
MEA01.02 Set performance and conformance targets.	A						R	R	R	R	R
MEA01.03 Collect and process performance and conformance data.					A		R	R	R	R	R
MEA01.04 Analyze and report performance.					A		R	R	R	R	R
MEA01.05 Ensure the implementation of corrective actions.					A		R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
MEA01.01 Establish a monitoring approach.	EDM05.01	• Evaluation of enterprise reporting requirements • Reporting and communications principles	Approved monitoring goals and metrics	Internal
			Monitoring requirements	Internal
	EDM05.02	Rules for validating and approving mandatory reports		
	EDM05.03	Assessment of reporting effectiveness		
MEA01.02 Set performance and conformance targets.	APO01.11	Performance goals and metrics for process improvement tracking	Monitoring targets	All APO; All BAI; All DSS; All MEA

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
MEA01.03 Collect and process performance and conformance data.	APO01.11	Process capability assessments	Processed monitoring data	Internal
	APO05.03	Investment portfolio performance reports		
	APO09.04	Service level performance reports		
	APO10.05	Results of vendor-compliance monitoring review		
	BAI01.06	Results of program performance reviews		
	BAI04.04	Availability, performance and capacity-monitoring review reports		
	BAI05.05	Success measures and results		
	DSS01.05	Facilities assessment reports		
	DSS02.07	• Incident status and trends report • Request fulfilment status and trends report		
MEA01.04 Analyze and report performance.			Performance reports	All APO; All BAI; All DSS; All MEA; EDM01.03
MEA01.05 Ensure the implementation of corrective actions.	APO01.09	Noncompliance remedial actions	Remedial actions and assignments	All APO; All BAI; All DSS; All MEA
	EDM05.02	Escalation guidelines	Status and results of actions	EDM01.03

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 13): Inputs and Outputs; 3.3 Selection (Task 2): Inputsand Outputs; 3.7 Monitoring (Task 1, Task 3): Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Conformance review	Skills Framework for the Information Age V6, 2015	CORE
ICT quality management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.6. ICT Quality Management
Quality assurance	Skills Framework for the Information Age V6, 2015	QUAS

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Self-assessment policy	Provides guidance for management's responsibilities in assessing operations as part of the continuous improvement program. Often used to report internally to executives or board on current capabilities, progress and improvement, based on business requirements. Assessments may be used during or after a process improvement program (i.e., to assess progress after completing an improvement).		
Whistle-blower policy	Encourages employees to raise concerns and questions in full confidence. Ensures employees that they will receive a response and be able to escalate concerns if they are not satisfied with the response. Assures that employees are protected when they raise issues and should not fear reprisal.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
To achieve the organization's goals and optimize performance, promote a culture of continuous improvement of business and I&T processes.		

G. Component: Services, Infrastructure and Applications
• Performance measurement system (e.g., balanced scorecard, skills management tools) • Self-assessment tools

Domain: Monitor, Evaluate and Assess Management Objective: MEA02 — Managed System of Internal Control	Focus Area: COBIT Core Model

Description

Continuously monitor and evaluate the control environment, including self-assessments and self-awareness. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize and maintain standards for internal control assessment and process control effectiveness.

Purpose

Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG03 Compliance with external laws and regulations • EG11 Compliance with internal policies	AG11 I&T compliance with internal policies
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG03 a. Cost of regulatory noncompliance, including settlements and fines b. Number of regulatory noncompliance issues causing public comment or negative publicity c. Number of noncompliance matters noted by regulators d. Number of regulatory noncompliance issues relating to contractual agreements with business partners	AG11 a. Number of incidents related to noncompliance with I&T-related policies b. Number of exceptions to internal policies c. Frequency of policy review and update
EG11 a. Number of incidents related to noncompliance to policy b. Percent of stakeholders who understand policies c. Percent of policies supported by effective standards and working practices	

A. Component: Process

Management Practice	Example Metrics
MEA02.01 Monitor internal controls. Continuously monitor, benchmark and improve the I&T control environment and control framework to meet organizational objectives.	a. Number of major internal control breaches b. Percent of controls environment and framework continuously monitored, benchmarked and improved to meet organizational objectives

Activities	Capability Level
1. Identify the boundaries of the internal control system. For example, consider how organizational internal controls take into account outsourced and/or offshore development or production activities.	3
2. Assess the status of external service providers' internal controls. Confirm that service providers comply with legal and regulatory requirements and contractual obligations.	
3. Perform internal control monitoring and evaluation activities based on organizational governance standards and industry-accepted frameworks and practices. Also include monitoring and evaluation of the efficiency and effectiveness of managerial supervisory activities.	
4. Ensure that control exceptions are promptly reported, followed up and analyzed, and appropriate corrective actions are prioritized and implemented according to the risk management profile (e.g., classify certain exceptions as a key risk and others as a non-key risk).	
5. Consider independent evaluations of the internal control system (e.g., by internal audit or peers).	
6. Maintain the internal control system, considering ongoing changes in business and I&T risk, the organizational control environment, and relevant business and I&T processes. If gaps exist, evaluate and recommend changes.	4
7. Regularly evaluate the performance of the control framework, benchmarking against industry accepted standards and good practices. Consider formal adoption of a continuous improvement approach to internal control monitoring.	5

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	09.10 Monitoring
ISO/IEC 38502:2017(E)	5.5 Governance and internal control
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.3 Audit and accountability (AU-2)
Management Practice	**Example Metrics**
MEA02.02 Review effectiveness of business process controls. Review the operation of controls, including monitoring and test evidence, to ensure that controls within business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing, continuous monitoring, independent assessments, command and control centers, and network operation centers. This evidence assures the enterprise that controls meet requirements related to business, regulatory and social responsibilities.	a. Number of weaknesses identified by external qualification and certification reports b. Number of controls being monitored and tested to ensure that controls within business processes operate effectively

Activities	Capability Level
1. Understand and prioritize risk to organizational objectives.	3
2. Identify key controls and develop a strategy suitable for validating controls.	
3. Identify information that will indicate whether the internal control environment is operating effectively.	
4. Maintain evidence of control effectiveness.	4
5. Develop and implement cost-effective procedures to obtain this information in line with applicable information quality criteria.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	
Management Practice	**Example Metrics**
MEA02.03 Perform control self-assessments. Encourage management and process owners to improve controls proactively through a continuing program of self-assessment that evaluates the completeness and effectiveness of management's control over processes, policies and contracts.	a. Number of self-assessments performed b. Number of identified gaps in self-assessments vs. industry standards or good practices

Activities	Capability Level
1. Define an agreed, consistent approach for performing control self-assessments and coordinating with internal and external auditors.	3
2. Maintain evaluation plans, and scope and identify evaluation criteria for conducting self-assessments. Plan the communication of results of the self-assessment process to business, IT and general management and the board. Consider internal audit standards in the design of self-assessments.	
3. Determine the frequency of periodic self-assessments, considering the overall effectiveness and efficiency of ongoing monitoring.	
4. Assign responsibility for self-assessment to appropriate individuals to ensure objectivity and competence.	
5. Provide for independent reviews to ensure objectivity of the self-assessment and enable the sharing of internal control good practices from other enterprises.	
6. Compare the results of the self-assessments against industry standards and good practices.	4
7. Summarize and report outcomes of self-assessments and benchmarking for remedial actions.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 27001:2013/Cor.2:2015(E)	9.3 Management review
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.7 Monitoring (Task 2)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
MEA02.04 Identify and report control deficiencies. Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.	a. Time between internal control deficiency occurrence and reporting b. Time between exception identification and agreed actions addressed c. Percent of implementation of remedial actions arising from control assessments

Activities	Capability Level
1. Communicate procedures for escalation of control exceptions, root cause analysis, and reporting to process owners and I&T stakeholders.	3
2. Consider related enterprise risk to establish thresholds for escalation of control exceptions and breakdowns.	
3. Identify, report and log control exceptions. Assign responsibility for resolving them and reporting on the status.	
4. Decide which control exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated. Inform affected process owners and stakeholders.	
5. Follow up on all exceptions to ensure that agreed-on actions have been addressed.	4
6. Identify, initiate, track and implement remedial actions arising from control assessments and reporting.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

B. Component: Organizational Structures

Key Management Practice	Chief Financial Officer	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	I&T Governance Board	Business Process Owners	Project Management Office	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
MEA02.01 Monitor internal controls.		R	A	R		R	R	R	R	R	R	R	R	R
MEA02.02 Review effectiveness of business process controls.	R		A	R	R	R								
MEA02.03 Perform control self-assessments.		R	A	R		R	R	R	R	R	R	R	R	R
MEA02.04 Identify and report control deficiencies.			A	R		R	R	R	R	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
MEA02.01 Monitor internal controls.	**From**	**Description**	**Description**	**To**
	APO12.04	Results of third-party risk assessments	Results of benchmarking and other evaluations	All APO; All BAI; All DSS; All MEA; EDM01.03
	APO13.03	Information security management system (ISMS) audit reports	Results of internal control monitoring and reviews	All APO; All BAI; All DSS; All MEA; EDM01.03
	Outside COBIT	Industry standards and good practices		
MEA02.02 Review effectiveness of business process controls.	BAI05.06	Compliance audit results	Evidence of control effectiveness	Internal
	BAI05.07	Reviews of operational use		
MEA02.03 Perform control self-assessments.			Self-assessment plans and criteria	All APO; All BAI; All DSS; All MEA
			Results of reviews of self-assessments	All APO; All BAI; All DSS; All MEA; EDM01.03
			Results of self-assessments	Internal
MEA02.04 Identify and report control deficiencies.	APO11.03	Root causes of failure to deliver quality	Remedial actions	All APO; All BAI; All DSS; All MEA
	APO12.06	Risk-related root causes	Control deficiencies	All APO; All BAI; All DSS; All MEA
	DSS06.01	• Results of processing effectiveness reviews • Root cause analyses and recommendations		
	DSS06.04	Evidence of error correction and remediation		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.7 Monitoring (Task 2): Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Risk management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Internal control policy	Communicates management's internal control objectives. Establishes standards for the design and operation of the enterprise system of internal controls to reduce exposure to all risk. Provides guidance for continuously monitoring and evaluating the control environment, including self-awareness and self-assessments.		
Internal control self-assessment guidance	Recommends continuous monitoring of internal controls to identify deficiencies and gaps in effectiveness, determine their root causes, and initiate plans of action and corrective milestones for reporting to stakeholders.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote awareness of the importance of an effective control environment. Encourage a proactive risk- and self-aware culture, including commitment to self-assessment and independent assurance reviews.		

G. Component: Services, Infrastructure and Applications
• COBIT and related products/tools • Third-party internal control assessment services

Page intentionally left blank

Domain: Monitor, Evaluate and Assess Management Objective: MEA03 — Managed Compliance With External Requirements	Focus Area: COBIT Core Model

Description

Evaluate that I&T processes and I&T-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with; integrate IT compliance with overall enterprise compliance.

Purpose

Ensure that the enterprise is compliant with all applicable external requirements.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
EG03 Compliance with external laws and regulations	AG01 I&T compliance and support for business compliance with external laws and regulations
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG03 a. Cost of regulatory noncompliance, including settlements and fines b. Number of regulatory noncompliance issues causing public comment or negative publicity c. Number of noncompliance matters noted by regulators d. Number of regulatory noncompliance issues relating to contractual agreements with business partners	AG01 a. Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss b. Number of IT-related noncompliance issues reported to the board, or causing public comment or embarrassment c. Number of noncompliance issues relating to contractual agreements with IT service providers

A. Component: Process

Management Practice	Example Metrics
MEA03.01 Identify external compliance requirements. On a continuous basis, monitor changes in local and international laws, regulations and other external requirements and identify mandates for compliance from an I&T perspective.	a. Frequency of compliance requirements reviews b. Percent of satisfaction of key stakeholders in regulatory review compliance process

Activities	Capability Level
1. Assign responsibility for identifying and monitoring any changes of legal, regulatory and other external contractual requirements relevant to the use of IT resources and the processing of information within the business and IT operations of the enterprise.	2
2. Identify and assess all potential compliance requirements and the impact on I&T activities in areas such as data flow, privacy, internal controls, financial reporting, industry-specific regulations, intellectual property, health and safety.	
3. Assess the impact of I&T-related legal and regulatory requirements on third-party contracts related to IT operations, service providers and business trading partners.	
4. Define the consequences of noncompliance.	
5. Obtain independent counsel, where appropriate, on changes to applicable laws, regulations and standards.	3
6. Maintain an up-to-date log of all relevant legal, regulatory and contractual requirements; their impact and required actions.	
7. Maintain a harmonized and integrated overall register of external compliance requirements for the enterprise.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	BC.RR Determine Legal / Regulatory Requirements
HITRUST CSF version 9, September 2017	06.01 Compliance with Legal Requirements
ISF, The Standard of Good Practice for Information Security 2016	SM2.3 Legal and Regulatory Compliance

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
MEA03.02 Optimize response to external requirements. Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider adopting and adapting industry standards, codes of good practice, and good practice guidance.	a. Average time between identifying external compliance issues and resolution b. Percent of satisfaction of relevant personnel with communication of new and changed regulatory compliance requirements

Activities	Capability Level
1. Regularly review and adjust policies, principles, standards, procedures and methodologies for their effectiveness in ensuring necessary compliance and addressing enterprise risk. Use internal and external experts, as required.	3
2. Communicate new and changed requirements to all relevant personnel.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas - Principle 13

Management Practice	Example Metrics
MEA03.03 Confirm external compliance. Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements.	a. Number of critical noncompliance issues identified per year b. Percent of process owners signing off, confirming compliance

Activities	Capability Level
1. Regularly evaluate organizational policies, standards, procedures and methodologies in all functions of the enterprise to ensure compliance with relevant legal and regulatory requirements in relation to the processing of information.	3
2. Address compliance gaps in policies, standards and procedures on a timely basis.	
3. Periodically evaluate business and IT processes and activities to ensure adherence to applicable legal, regulatory and contractual requirements.	
4. Regularly review for recurring patterns of compliance failures and assess lessons learned.	4
5. Based on review and lessons learned, improve policies, standards, procedures, methodologies, and associated processes and activities.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
MEA03.04 Obtain assurance of external compliance. Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.	a. Number of compliance reports obtained b. Percent of service provider compliance based on independent reviews c. Time between identification of compliance gap and corrective action d. Number of corrective action reports addressing compliance gaps closed in a timely manner

Activities	Capability Level
1. Obtain regular confirmation of compliance with internal policies from business and IT process owners and unit heads.	2
2. Perform regular (and, where appropriate, independent) internal and external reviews to assess levels of compliance.	
3. If required, obtain assertions from third-party I&T service providers on levels of their compliance with applicable laws and regulations.	
4. If required, obtain assertions from business partners on levels of their compliance with applicable laws and regulations as they relate to intercompany electronic transactions.	
5. Integrate reporting on legal, regulatory and contractual requirements at an enterprisewide level, involving all business units.	3
6. Monitor and report on noncompliance issues and, where necessary, investigate the root cause.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Quality Assurance
ISO/IEC 27002:2013/Cor.2:2015(E)	18. Compliance

B. Component: Organizational Structures

Key Management Practice	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Chief Information Officer	I&T Governance Board	Business Process Owners	Project Management Office	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer	Legal Counsel	Compliance	Audit
MEA03.01 Identify external compliance requirements.				R		R								R	R	A	R
MEA03.02 Optimize response to external requirements.	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	A
MEA03.03 Confirm external compliance.	R	R	R	R	R	R								R	R	A	
MEA03.04 Obtain assurance of external compliance.				R											R	A	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

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

Management Practice	Inputs		Outputs	
	From	Description	Description	To
MEA03.01 Identify external compliance requirements.	Outside COBIT	Legal and regulatory compliance requirements	Log of required compliance actions	Internal
			Compliance requirements register	Internal
MEA03.02 Optimize response to external requirements.			Communications of changed compliance requirements	All APO; All BAI; All DSS; All MEA; EDM01.01
			Updated policies, principles, procedures and standards	APO01.09; APO01.11
MEA03.03 Confirm external compliance.	BAI05.06	Compliance audit results	Compliance confirmations	EDM01.03
	BAI09.05	Results of installed license audits	Identified compliance gaps	MEA04.08
	BAI10.05	License deviations		
	DSS01.04	Insurance policy reports		
MEA03.04 Obtain assurance of external compliance.	EDM05.02	Rules for validating and approving mandatory reports	Compliance assurance reports	EDM01.03
	EDM05.03	Assessment of reporting effectiveness	Reports of noncompliance issues and root causes	EDM01.03; MEA04.04

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

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

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Compliance policy	Identifies regulatory, contractual and internal compliance requirements. Explains the process to assess compliance with regulatory, contractual and internal requirements. Lists roles and responsibilities for different activities in the process and provides guidance on metrics to measure compliance. Obtains compliance reports and confirms compliance or corrective actions to address remediation of compliance gaps in a timely manner.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote a compliance-aware culture, including zero tolerance of noncompliance with legal and regulatory requirements.		

G. Component: Services, Infrastructure and Applications
• Regulatory Watch services • Third-party compliance assessment services

Domain: Monitor, Evaluate and Assess Management Objective: MEA04 — Managed Assurance	Focus Area: COBIT Core Model

Description

Plan, scope and execute assurance initiatives to comply with internal requirements, laws, regulations and strategic objectives. Enable management to deliver adequate and sustainable assurance in the enterprise by performing independent assurance reviews and activities.

Purpose

Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

The management objective supports the achievement of a set of primary enterprise and alignment goals:

Enterprise Goals	Alignment Goals
• EG03 Compliance with external laws and regulations • EG11 Compliance with internal policies	AG11 I&T compliance with internal policies
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG03 a. Cost of regulatory noncompliance, including settlements and fines b. Number of regulatory noncompliance issues causing public comment or negative publicity c. Number of noncompliance matters noted by regulators d. Number of regulatory noncompliance issues relating to contractual agreements with business partners	AG11 a. Number of incidents related to noncompliance with I&T-related policies b. Number of exceptions to internal policies c. Frequency of policy review and update
EG11 a. Number of incidents related to noncompliance to policy b. Percent of stakeholders who understand policies c. Percent of policies supported by effective standards and working practices	

A. Component: Process

Management Practice	Example Metrics
MEA04.01 Ensure that assurance providers are independent and qualified. Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.	a. Percent of processes receiving independent review b. Percent of qualifications and competencies met by service providers

Activities	Capability Level
1. Establish adherence to applicable codes of ethics and standards (e.g., Code of Professional Ethics of ISACA) and (industry- and geography-specific) assurance standards (e.g., IT Audit and Assurance Standards of ISACA and the International Auditing and Assurance Standards Board's [IAASB's] International Framework for Assurance Engagements [IAASB Assurance Framework]).	2
2. Establish independence of assurance providers.	
3. Establish competency and qualification of assurance providers.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
HITRUST CSF version 9, September 2017	06.03 Information System Audit Considerations

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
MEA04.02 Develop risk-based planning of assurance initiatives. Determine assurance objectives based on assessments of the internal and external environment and context, the risk of not achieving enterprise goals, and the opportunities associated achievement of the same goals.	a. Percent of assurance initiatives following approved assurance program and plan standards b. Percent of assurance plan initiatives based on risk
Activities	**Capability Level**
1. Understand the enterprise strategy and priorities.	2
2. Understand the internal context of the enterprise. This understanding will help the assurance professional to better assess the enterprise goals and the relative importance of enterprise and alignment goals, as well as the most important threats to these goals. In turn, this will assist in defining a better and more relevant scope for the assurance engagement.	
3. Understand the external context of the enterprise. This understanding will help the assurance professional to better understand the enterprise goals and the relative importance of enterprise and alignment goals, as well as the most important threats to these goals. In turn, this will assist in defining a better and more relevant scope for the assurance engagement.	
4. Develop an overall yearly plan for assurance initiatives containing the consolidated assurance objectives.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas—Principle 15
Management Practice	**Example Metrics**
MEA04.03 Determine the objectives of the assurance initiative. Define and agree with all stakeholders on the objectives of the assurance initiative.	a. Percent of objectives achieved through the assurance initiative b. Percent of stakeholder satisfaction with the assurance initiative's objectives
Activities	**Capability Level**
1. Define the assurance objective of the assurance initiative by identifying the stakeholders of the assurance initiative and their interests.	2
2. Agree on the high-level objectives and the organizational boundaries of the assurance engagement.	
3. Consider the use of the COBIT Goals Cascade and its different levels to express the assurance objective.	3
4. Ensure that the objectives of the assurance engagement consider all three value objective components: delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Quality Assurance
Management Practice	**Example Metrics**
MEA04.04 Define the scope of the assurance initiative. Define and agree with all stakeholders on the scope of the assurance initiative, based on the assurance objectives.	a. Number of engagement plans, based on the scope, that consider information to be collected and stakeholders to be interviewed b. Percent of stakeholder satisfaction with the scope of the assurance initiative, based on the assurance objectives
Activities	**Capability Level**
1. Define all governance components in scope of the review, that is, the principles, policies and frameworks; processes; organizational structures; culture, ethics and behavior; information; services, infrastructure and applications; people, skills and competences	2
2. Based on the scope definition, define an engagement plan, considering information to be collected and stakeholders to be interviewed.	3
3. Confirm and refine the scope based on an understanding of the enterprise architecture.	
4. Refine the scope of the assurance engagement, based on available resources.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	TP.LA Apply Logging and Audit Processes

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
MEA04.05 Define the work program for the assurance initiative. Define a detailed work program for the assurance initiative, structured according to the management objectives and governance components in scope.	a. Percent of management controls identified as weak without defined practices to reduce residual risk b. Number of controls reviewed c. Percent of stakeholder satisfaction with the work program for the assurance initiative

Activities	Capability Level
1. Define detailed steps for collecting and evaluating information from management controls within scope. Focus on assessing the definition and application of good practices, related to control design, and achievement of control objectives, related to control effectiveness.	2
2. Understand the context of the management objectives and the supporting management controls that are put in place. Understand how these management controls contribute to the achievement of the alignment goals and enterprise goals.	
3. Understand all stakeholders and their interests.	
4. Agree on the expected good practices for the management controls.	3
5. Should a management control be weak, define practices to identify residual risk (in preparation for reporting).	
6. Understand the life cycle stage of the management controls and agree on expected values.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
MEA04.06 Execute the assurance initiative, focusing on design effectiveness. Execute the planned assurance initiative. Validate and confirm the design of the internal controls in place. Additionally, and specifically in internal audit assignments, consider the cost-effectiveness of the governance component design.	a. Percent of assurance initiatives that consider cost effectiveness of design b. Percent of stakeholder satisfaction with the design of the assurance initiative

Activities	Capability Level
1. Refine the understanding of the IT assurance subject.	2
2. Refine the scope of the IT assurance subject.	
3. Observe/inspect and review the management control approach. Validate the design with the control owner for completeness, relevancy, timeliness and measurability.	3
4. Ask the control owner whether the responsibilities for the governance component and overall accountability have been assigned. Confirm the response. Test whether accountability and responsibilities are understood and accepted. Verify that the right skills and the necessary resources are available.	
5. Reconsider the balance of prevention vs. detection and correction types of management control activities.	
6. Consider the effort spent in maintaining the management controls and the associated cost/effectiveness.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SI1 Security Audit
ISO/IEC 27001:2013/Cor.2:2015(E)	9.2 Internal audit

Management Practice	Example Metrics
MEA04.07 Execute the assurance initiative, focusing on operating effectiveness. Execute the planned assurance initiative. Test whether the internal controls in place are appropriate and sufficient. Test the outcome of the key management objectives in scope of the assurance initiative.	a. Percent of assurance initiatives that test the outcome of key, in-scope management objectives b. Percent of stakeholder satisfaction with the execution of the assurance initiative

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Assess whether the expected outcomes for each of the management controls in scope are achieved. That is, assess the effectiveness of the management control (control effectiveness).	3
2. Ensure that the assurance professional tests the outcome or effectiveness of the management control by looking for direct and indirect evidence of the impact on the management controls goals. This implies the direct and indirect substantiation of measurable contribution of the management goals to the alignment goals, thereby recording direct and indirect evidence of actually achieving the expected outcomes.	
3. Determine whether the assurance professional obtains direct or indirect evidence for selected items/periods by applying a selection of testing techniques to ensure that the management control under review is working effectively. Ensure that the assurance professional also performs a limited review of the adequacy of the management control results and determines the level of substantive testing and additional work needed to provide assurance that the management control performance is adequate.	
4. Investigate whether a management control can be made more efficient and if its design can be more effective by optimizing steps or looking for synergies with other management controls.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SI1 Security Audit
SO/IEC 27001:2013/Cor.2:2015(E)	9.2 Internal audit
Management Practice	**Example Metrics**
MEA04.08 Report and follow up on the assurance initiative. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control weaknesses.	a. Stakeholder acceptance of the assurance report b. Stakeholder acceptance of recommendations for improvement relating to identified operational performance, external compliance and internal control weaknesses
Activities	**Capability Level**
1. Document the impact of control weaknesses.	2
2. Communicate with management during execution of the initiative so there is a clear understanding of the work performed and agreement on and acceptance of the preliminary findings and recommendations.	
3. Provide management with a report (aligned with the terms of reference, scope and agreed reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	3
4. Supervise the assurance activities and make sure the work done is complete, meets objectives and is of an acceptable quality. Revise the approach or detailed steps if quality gaps occur.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
MEA04.09 Follow up on recommendations and actions. Agree on, follow up and implement the identified recommendations for improvement.	a. Number of recurring weaknesses b. Number of identified weaknesses resolved
Activities	**Capability Level**
1. Agree on and implement internally, within the organization, the necessary actions that need to be taken to resolve identified weaknesses and gaps.	2
2. Follow up, within the organization, to determine whether corrective actions were taken and internal control weaknesses were resolved.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures														
Key Management Practice	Chief Operating Officer	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Enterprise Risk Committee	Business Process Owners	Data Management Function	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager	Legal Counsel	Audit
MEA04.01 Ensure that assurance providers are independent and qualified.			R	R	R	R						R	A
MEA04.02 Develop risk-based planning of assurance initiatives.	R	R	R	R		R						R	A
MEA04.03 Determine the objectives of the assurance initiative.	R	R	R	R		R						R	A
MEA04.04 Define the scope of the assurance initiative.	R	R	R	R		R						R	A
MEA04.05 Define the work program for the assurance initiative.	R		R	R		R						R	A
MEA04.06 Execute the assurance initiative, focusing on design effectiveness.	R		R	R		R	R	R	R	R	R	R	A
MEA04.07 Execute the assurance initiative, focusing on operating effectiveness.	R		R	R		R	R	R	R	R	R	R	A
MEA04.08 Report and follow up on the assurance initiative.	R		R	R		R						R	A
MEA04.09 Follow up on recommendations and actions.	R	R	A	R		R		R				R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
MEA04.01 Ensure that assurance providers are independent and qualified.			Results of assurance provider evaluations	Internal
MEA04.02 Develop risk-based planning of assurance initiatives.	BAI01.05	Program audit plans	Assurance plans	All APO; All BAI; All DSS; All MEA; EDM01.03
	DSS01.02	Independent assurance plans	Assessment criteria	Internal
			High-level assessments	Internal
MEA04.03 Determine the objectives of the assurance initiative.	MEA04.02	Assurance plans	Assurance objectives and expected benefits	Internal
MEA04.04 Define the scope of the assurance initiative.	APO11.03	Root causes of failure to deliver quality	Assurance review practices	Internal
	APO12.06	Risk-related root causes	Engagement plan	Internal
	DSS06.01	Root cause analyses and recommendations		
	MEA03.04	Reports of noncompliance issues and root causes	Assurance review scope	Internal

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
MEA04.05 Define the work program for the assurance initiative.	**From**	**Description**	**Description**	**To**
	APO12.04	Risk analysis and risk profile reports for stakeholders	Refined scope	Internal
			Detailed assurance work program	MEA04.06
MEA04.06 Execute the assurance initiative, focusing on design effectiveness.	APO12.06	Risk-related root causes	Documented design of internal controls	MEA04.07
	DSS06.01	Root cause analyses and recommendations		
	MEA04.05	Detailed assurance work program		
MEA04.07 Execute the assurance initiative, focusing on operating effectiveness.	DSS02.02	Incident and service request log	Control effectiveness testing	MEA04.08; MEA04.09
	DSS02.05	Incident resolutions		
	DSS03.05	Problem resolution monitoring reports		
	DSS05.02	Results of penetration tests		
	DSS05.05	Access logs		
	DSS06.01	Root cause analyses and recommendations		
	MEA04.06	Documented design of internal controls		
MEA04.08 Report and follow up on the assurance initiative.	MEA03.03	Identified compliance gaps	Assurance review report	All APO; All BAI; All DSS; All MEA; EDM05.03
	MEA04.07	Control effectiveness testing	Assurance review results	All APO; All BAI; All DSS; All MEA; EDM05.03; MEA04.09
MEA04.09 Follow up on recommendations and actions.	MEA04.07	Control effectiveness testing	Remedial actions	All APO; All BAI; All DSS; All MEA
	MEA04.08	Assurance review results		
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
A number of core principles, described by the Institute of Internal Auditors®, support the effectiveness and efficiency of the (internal) audit function. These principles include, among others, the importance of independence, effective communication skills, proactiveness, etc.	Core Principles for the Professional Practice of Internal Auditing, The Institute of Internal Auditors	cfr. IIA website—Standards & Guidance - Core Principles
Risk management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Assurance guide	Provides guidance on performing assurance activities. Enables efficient and effective development of I&T assurance initiatives, including planning, scoping and executing assurance reviews, based on well-accepted assurance approaches. Provides assurance steps to test the control design, test the outcome of the operational effectiveness of the control, and document control weaknesses and their impact.		
Internal audit charter	Provides independence to undertake audit reviews and report findings and recommendations directly to top management. The internal audit function should be a separate entity reporting either to the chief executive officer or chief operating officer. With respect to I&T, the charter should stipulate that the function is responsible for reviewing both general and application controls to determine whether the controls have been designed in accordance with management direction, established standards and procedures, and known legal requirements, and whether the controls are operating effectively to provide reliability and security over the data being processed (i.e., confidentiality, integrity and availability). The charter should stipulate that the internal audit function is responsible for reviewing the design, development and implementation of new systems or major modifications of existing systems.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture that embraces internal audit and assurance findings and recommendations, based on root cause analysis. Leaders must ensure that internal audit and assurance are involved in strategic initiatives and recognize the need for (and value of) audit and assurance reports.		
Ensure an ethical culture of internal auditing through an appropriate code of ethics.	Code of Ethics, The Institute of Internal Auditors	cfr. IIA website—Standards & Guidance—Code of Ethics

G. Component: Services, Infrastructure and Applications
• Assurance engagement tools • Event log auditing tools • Third-party assurance provisioning services

Appendices

A.1 Appendix A: Goals Cascade—Mapping Tables

The mapping tables in Appendix A inform the goals cascade. The first table maps alignment goals to enterprise goals; the second table maps governance and management objectives to alignment goals. The "P" in the table refers to primary and the "S" refers to secondary.

A.1.1 Mapping Table: Enterprise Goals—Alignment Goals

Figure A.1—Mapping Enterprise Goals and Alignment Goals

		EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
		Portfolio of competitive products and services	Managed business risk	Compliance with external laws and regulations	Quality of financial information	Customer-oriented service culture	Business service continuity and availability	Quality of management information	Optimization of internal business process functionality	Optimization of business process costs	Staff skills, motivation and productivity	Compliance with internal policies	Managed digital transformation programs	Product and business innovation
AG01	I&T compliance and support for business compliance with external laws and regulations		S	P								S		
AG02	Managed I&T-related risk		P				S							
AG03	Realized benefits from I&T-enabled investments and services portfolio	S				S			S	S			P	
AG04	Quality of technology-related financial information				P			P		P				
AG05	Delivery of I&T services in line with business requirements	P				S	S		S				S	
AG06	Agility to turn business requirements into operational solutions	P				S			S				S	S
AG07	Security of information, processing infrastructure and applications, and privacy		P				P							
AG08	Enabling and supporting business processes by integrating applications and technology	P				P			S		S		P	S
AG09	Delivering programs on time, on budget and meeting requirements and quality standards	P				S			S	S			P	S
AG10	Quality of I&T management information				P			P		S				
AG11	I&T compliance with internal policies		S	P								P		
AG12	Competent and motivated staff with mutual understanding of technology and business					S					P			
AG13	Knowledge, expertise and initiatives for business innovation	P		S									S	P

A.1.2 Mapping Table: Alignment Goals—Governance and Management Objectives

Figure—A.2 Mapping Governance and Management Objectives to Alignment Goals

		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		I&T compliance and support for business compliance with external laws and regulations	Managed I&T-related risk	Realized benefits from I&T-enabled investments and services portfolio	Quality of technology-related financial information	Delivery of I&T services in line with business requirements	Agility to turn business requirements into operational solutions	Security of information, processing infrastructure and applications, and privacy	Enabling and supporting business processes by integrating applications and technology	Delivering programs on time, on budget and meeting requirements and quality standards	Quality of I&T management information	I&T compliance with internal policies	Competent and motivated staff with mutual understanding of technology and business	Knowledge, expertise and initiatives for business innovation
EDM01	Ensured governance framework setting and maintenance	P	S	P					S			S		
EDM02	Ensured benefits delivery			P		S	S		S					S
EDM03	Ensured risk optimization	S	P					P				S		
EDM04	Ensured resource optimization			S		S	S		S	P			S	
EDM05	Ensured stakeholder engagement				S						P	S		
APO01	Managed I&T management framework	S	S	P		S		S	S	S	S	P		
APO02	Managed strategy			S		S	S		P				S	S
APO03	Managed enterprise architecture			S		S	P	S	P					
APO04	Managed innovation			S			P		S				S	P
APO05	Managed portfolio			P		P	S		S	S				
APO06	Managed budget and costs			S	P					P	S			
APO07	Managed human resources			S		S				S			P	P
APO08	Managed relationships			S		P	P		S	S			P	P
APO09	Managed service agreements					P			S					
APO10	Managed vendors					P	S			S				
APO11	Managed quality			S	S	S				P	P			
APO12	Managed risk		P					P						
APO13	Managed security	S	S					P						
APO14	Managed data	S	S		S			S			P			
BAI01	Managed programs			P			S		S	P				
BAI02	Managed requirements definition			S		P	P		S	P			S	
BAI03	Managed solutions identification and build			S		P	P		S	P				
BAI04	Managed availability and capacity					P		S		S				
BAI05	Managed organizational changes			P		S	S		P	P			S	
BAI06	Managed IT changes		S			S	P		S					
BAI07	Managed IT change acceptance and transitioning		S				P			S				
BAI08	Managed knowledge			S			S		S	S			P	P
BAI09	Managed assets				P						S			
BAI10	Managed configuration					S		P						
BAI11	Managed projects			P		S	P			P				
DSS01	Managed operations					P			S					
DSS02	Managed service requests and incidents		S			P		S						
DSS03	Managed problems		S			P		S						
DSS04	Managed continuity		S			P		P						
DSS05	Managed security services	S	P			S		P				S		
DSS06	Managed business process controls		S			S		S	P			S		
MEA01	Managed performance and conformance monitoring	S		S		P				S	P	S		
MEA02	Managed system of internal control	S	S		S	S		S		S	S	P		
MEA03	Managed compliance with external requirements	P										S		
MEA04	Managed assurance	S	S		S	S		S			S	P		

A.2 Appendix B: Organizational Structures—Overview and Descriptions

Throughout the detailed guidance in Chapter 4, the organizational structures components draw from the roles and structures outlined in **figure A.3** (see also section 3.5 for an overview of the organizational structures component).

Across enterprises, the nomenclature applied to each role or structure will likely differ. Based on the descriptions below, each enterprise may identify appropriate roles and structures—given its own business context, organization, and operating environment—and assign levels of accountability and responsibility accordingly.

Figure A.3—COBIT Roles and Organizational Structures

Role/Structure	Description
Board	Group of the most senior executives and/or nonexecutive directors accountable for governance and overall control of enterprise resources
Executive Committee	Group of senior executives appointed by the board to ensure that the board is involved in, and kept informed of, major decisions (The executive committee is accountable for managing the portfolios of I&T-enabled investments, I&T services and I&T assets; ensuring that value is delivered; and managing risk. The committee is normally chaired by a board member.)
Chief Executive Officer	Highest-ranking officer charged with the total management of the enterprise
Chief Financial Officer	Most senior official accountable for all aspects of financial management, including financial risk and controls and reliable and accurate accounts
Chief Operating Officer	Most senior official accountable for operation of the enterprise
Chief Risk Officer	Most senior official accountable for all aspects of risk management across the enterprise (An I&T risk officer function may be established to oversee I&T-related risk.)
Chief Information Officer	Most senior official responsible for aligning IT and business strategies and accountable for planning, resourcing and managing delivery of I&T services and solutions
Chief Technology Officer	Most senior official tasked with technical aspects of I&T, including managing and monitoring decisions related to I&T services, solutions and infrastructures (This role may also be taken by the CIO.)
Chief Digital Officer	Most senior official tasked with putting into practice the digital ambition of the enterprise or business unit (This role may be taken by the CIO or another member of the executive committee.)
I&T Governance Board	Group of stakeholders and experts accountable for guiding I&T-related matters and decisions, including managing I&T-enabled investments, delivering value and monitoring risk
Architecture Board	Group of stakeholders and experts accountable for guiding enterprise architecture-related matters and decisions and for setting architectural policies and standards
Enterprise Risk Committee	Group of executives accountable for enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions (An I&T risk council may be established to consider I&T risk in more detail and advise the enterprise risk committee.)
Chief Information Security Officer	Most senior official accountable for all aspects of security management across the enterprise
Business Process Owner	Individual accountable for performing processes and/or realizing process objectives, driving process improvement and approving process changes
Portfolio Manager	Individual responsible for guiding portfolio management, ensuring selection of correct programs and projects, managing and monitoring programs and projects for optimal value, and realizing long-term strategic objectives effectively and efficiently
Steering (Programs/ Projects) Committee	Group of stakeholders and experts accountable for guiding programs and projects, including managing and monitoring plans, allocating resources, delivering benefits and value, and managing program and project risk
Program Manager	Individual responsible for guiding a specific program, including articulating and following up on goals and objectives of the program and managing risk and impact on the business

Figure A.3—COBIT Roles and Organizational Structures *(cont.)*	
Role/Structure	**Description**
Project Manager	Individual responsible for guiding a specific project, including coordinating and delegating time, budget, resources and tasks across the project team
Project Management Office	Function responsible for supporting program and project managers and for gathering, assessing and reporting information about the conduct of programs and constituent projects
Data Management Function	Function responsible for supporting enterprise data assets across the data life cycle and managing data strategy, infrastructure and repositories
Head Human Resources	Most senior official accountable for planning and policies regarding human resources in the enterprise
Relationship Manager	Senior individual responsible for overseeing and managing the internal interface and communications between business and I&T functions
Head Architect	Senior individual accountable for the enterprise architecture process
Head Development	Senior individual accountable for I&T–related solution development processes
Head IT Operations	Senior individual accountable for IT operational environments and infrastructure
Head IT Administration	Senior individual accountable for I&T–related records and responsible for supporting I&T–related administrative matters
Service Manager	Individual who manages the development, implementation, evaluation and ongoing maintenance of new and existing products and services for a specific customer (user) or group of customers (users)
Information Security Manager	Individual who manages, designs, oversees and/or assesses an enterprise's information security
Business Continuity Manager	Individual who manages, designs, oversees and/or assesses an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events
Privacy Officer	Individual responsible for monitoring risk and business impact of privacy laws and for guiding and coordinating the implementation of policies and activities that ensure compliance with privacy directives (In some enterprises, the position may be referenced as the data protection officer.)
Legal Counsel	Function responsible for guidance on legal and regulatory matters
Compliance	Function responsible for all guidance on external compliance
Audit	Function responsible for provision of internal audits

A.3 Appendix C: Detailed List of References

The following standards and guidance contribute to the detailed references to the 40 core COBIT® 2019 governance and management objectives.

- CIS® Center for Internet Security®, *The CIS Critical Security Controls for Effective Cyber Defense*, Version 6.1, August 2016
- CMMI® Cybermaturity Platform, 2018
- CMMI® Data Management Maturity (DMM)℠ model, 2014
- Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM) Framework, June 2017
- European Committee for Standardization (CEN), *e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework*, EN 16234-1:2016

- HITRUST® Common Security Framework, version 9, September 2017
- Information Security Forum (ISF), *The Standard of Good Practice for Information Security 2016*
- International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) standards
  - ISO/IEC 20000-1:2011(E)
  - ISO/IEC 27001:2013/Cor.2:2015(E)
  - ISO/IEC 27002:2013/Cor.2:2015(E)
  - ISO/IEC 27004:2016(E)
  - ISO/IEC 27005:2011(E)
  - ISO/IEC 38500:2015(E)
  - ISO/IEC 38502:2017(E)
- Information Technology Infrastructure Library (ITIL®) v3, 2011
- Institute of Internal Auditors® (IIA®), "Core Principles for the Professional Practice of Internal Auditing"• *King IV Report on Corporate Governance™*, 2016
- *King IV Report on Corporate Governance™*, 2016
- US National Institute of Standards and Technology (NIST) standards
  - *Framework for Improving Critical Infrastructure Cybersecurity* V1.1, April 2018
  - Special Publication 800-37, Revision 2 (Draft), May 2018
  - Special Publication 800-53, Revision 5 (Draft), August 2017
- *A Guide to the Project Management Body of Knowledge: PMBOK® Guide Sixth Edition*, 2017
- PROSCI® 3-Phase Change Management Process
- Scaled Agile Framework for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®) V6, 2015
- The Open Group IT4IT® Reference Architecture, version 2.0
- The Open Group Standard TOGAF® version 9.2, 2018

Page intentionally left blank