A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO07.04 Assess and recognize/reward employee job performance. Conduct timely, regular performance evaluations against individual objectives derived from enterprise goals, established standards, specific job responsibilities, and the skills and competency framework. Implement a remuneration/recognition process that rewards successful attainment of performance goals.	a. Number of official feedback moments and 360-degree evaluations performed b. Number and value of rewards given to staff

Activities	Capability Level
1. Consider functional/enterprise goals as the context for setting individual goals.	2
2. Set individual goals aligned with the relevant I&T and enterprise goals. Base goals on specific, measurable, achievable, relevant and time-bound (SMART) objectives that reflect core competencies, enterprise values and skills required for the role(s).	
3. Provide timely feedback regarding performance against the individual's goals.	
4. Provide specific instructions for the use and storage of personal information in the evaluation process, in compliance with applicable personal data and employment legislation.	
5. Compile 360-degree performance evaluation results.	3
6. Provide formal career planning and professional development plans based on the results of the evaluation process to encourage competency development and opportunities for personal advancement and to reduce dependence on key individuals. Provide employee coaching on performance and conduct whenever appropriate.	
7. Implement a remuneration/recognition process that rewards appropriate commitment, competency development and successful attainment of performance goals. Ensure that the process is applied consistently and in line with organizational policies.	
8. Implement and communicate a disciplinary process.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Develop

Management Practice	Example Metrics
APO07.05 Plan and track the usage of IT and business human resources. Understand and track the current and future demand for business and IT human resources with responsibilities for enterprise I&T. Identify shortfalls and provide input into sourcing plans, enterprise and IT recruitment processes, and business and IT recruitment processes.	a. Number of identified shortfalls and missing skills in planning for staffing b. Time spent per full-time equivalent (FTE) on assignments and projects

Activities	Capability Level
1. Create and maintain an inventory of business and IT human resources.	2
2. Understand the current and future demand for human resources to support the achievement of I&T objectives and to deliver services and solutions based on the portfolio of current I&T-related initiatives, the future investment portfolio and day-to-day operational needs.	3
3. Identify shortfalls and provide input into sourcing plans as well as enterprise and IT recruitment processes. Create and review the staffing plan, keeping track of actual usage.	
4. Maintain adequate information on the time spent on different tasks, assignments, services or projects.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Assess; Reward

Management Practice	Example Metrics
APO07.06 Manage contract staff. Ensure that consultants and contract personnel who support the enterprise with I&T skills know and comply with the organization's policies and meet agreed contractual requirements.	a. Percent of contractors signing off on the enterprise control framework b. Frequency of periodic reviews conducted to ensure correctness and compliance of contractor's staff

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Implement contract staff policies and procedures.	2
2. At the commencement of the contract, obtain formal agreement from contractors that they are required to comply with the enterprise's I&T control framework, such as policies for security clearance, physical and logical access control, use of facilities, information confidentiality requirements, and nondisclosure agreements.	
3. Advise contractors that management reserves the right to monitor and inspect all usage of IT resources, including email, voice communications, and all programs and data files.	
4. As part of their contracts, provide contractors with a clear definition of their roles and responsibilities, including explicit requirements to document their work to agreed standards and formats.	
5. Review contractors' work and base the approval of payments on the results.	
6. In formal and unambiguous contracts, define all work performed by external parties.	3
7. Conduct periodic reviews to ensure that contract staff have signed and agreed on all necessary agreements.	4
8. Conduct periodic reviews to ensure that contractors' roles and access rights are appropriate and in line with agreements.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Deploy

B. Component: Organizational Structures																	
Key Management Practice	**Chief Financial Officer**	**Chief Operating Officer**	**Chief Information Officer**	**Chief Technology Officer**	**Chief Digital Officer**	**Project Management Office**	**Head Human Resources**	**Head Architect**	**Head Development**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Business Continuity Manager**	**Privacy Officer**	**Legal Counsel**
APO07.01 Acquire and maintain adequate and appropriate staffing.			A	R	R	R	R	R	R	R	R	R	R	R		
APO07.02 Identify key IT personnel.			A	R	R	R	R	R	R	R	R	R	R	R	R	R
APO07.03 Maintain the skills and competencies of personnel.			A	R	R	R	R	R	R	R	R	R	R	R		
APO07.04 Assess and recognize/reward employee job performance.			A			R	R	R	R	R	R	R	R	R		
APO07.05 Plan and track the usage of IT and business human resources.	R	A	R	R	R	R	R	R	R	R	R	R	R	R		
APO07.06 Manage contract staff.			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**
APO07.01 Acquire and maintain adequate and appropriate staffing.	APO01.05	Definition of supervisory practices	Job descriptions and personnel sourcing plans	Internal
	APO06.03	• IT budget • Budget communications	Staffing requirement evaluations	Internal
	EDM04.01	• Guiding principles for allocating resources and capabilities • Approved resources plan	Competency and career development plans	Internal; APO07.02
	EDM04.03	Remedial actions to address resource management deviations		
	Outside COBIT	• Enterprise HR policies and procedures • Enterprise goals and objectives		
APO07.02 Identify key IT personnel.	APO07.01	Competency and career development plans	Job termination action plans	Internal
			Minimal amount of vacation guidance	Internal
APO07.03 Maintain the skills and competencies of personnel.	APO01.08	Target skills and competencies matrix	Skills and competencies matrix	APO01.05; APO14.01 BAI01.02; BAI01.04; BAI03.12
	BAI08.02	Published knowledge repositories	Skill development plans	APO01.05; EDM04.01
	BAI08.03	Knowledge awareness and training schemes	Review reports	Internal
	DSS04.06	• Training requirements • Monitoring results of skills and competencies		
	EDM01.02	Reward system approach		
	EDM04.03	Remedial actions to address resource management deviations		
	Outside COBIT	Enterprise goals and objectives		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO07.04 Assess and recognize/reward employee job performance.	**From**	**Description**	**Description**	**To**
	APO04.01	Recognition and reward program	Improvement plans	Internal
	BAI05.04	Aligned HR performance objectives	Performance evaluations	Internal
	BAI05.06	HR performance review results	Personnel goals	Internal
	DSS06.03	Allocated access rights		
	EDM01.02	Reward system approach		
	Outside COBIT	Enterprise goals and objectives		
APO07.05 Plan and track the usage of IT and business human resources.	APO06.02	Budget allocations	Inventory of business and IT human resources	BAI01.04
	BAI01.04	Resource requirements and roles	Resource utilization records	BAI01.06
	BAI11.08	Project resource requirements	Resourcing shortfall analyses	BAI01.06
	EDM04.02	Communication of resourcing strategies		
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities		
	Enterprise organization	Current and future portfolios		
	Outside COBIT	Enterprise organization structure		
APO07.06 Manage contract staff.	BAI01.04	Resource requirements and roles	Contract agreement reviews	Internal
	BAI01.09	Communication of program retirement and ongoing accountabilities	Contract agreements	Internal
	BAI11.08	Project resource requirements	Contract staff policies	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 9. Project resource management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Education and training provision	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.3. Education and Training Provision
Learning and development management	Skills Framework for the Information Age V6, 2015	ETMG
Performance management	Skills Framework for the Information Age V6, 2015	PEMT
Personnel development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.9. Personnel Development
Professional development	Skills Framework for the Information Age V6, 2015	PDSV
Resourcing	Skills Framework for the Information Age V6, 2015	RESC

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Contract staff policy	Enumerates criteria for augmenting staff with third-party consultants and/or contractors in accordance with enterprise IT procurement policy and the I&T control framework. Specifies what type of work can be performed or augmented by third parties, under what conditions, and when.	National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.16 Personnel security (PS-1)
Human resources (HR) policies	Outlines mutual expectations of the enterprise and its employees. Enumerates acceptable and unacceptable employee behaviors in a code of conduct to help manage risk related to human behavior.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Describe the roles and responsibilities of users toward information, media and network usage, security, and privacy. Encourage and communicate a common culture that prescribes expected behaviors for all individuals in the enterprise and establishes zero tolerance for unethical behaviors.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5, August 2017	3.14 Planning (PL-4)

G. Component: Services, Infrastructure and Applications
• HR management system • Performance measurement system (e.g., balanced scorecard, skills management tools) • Resource planning tools

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO08 — Managed Relationships	Focus Area: COBIT Core Model

Description

Manage relationships with business stakeholders in a formalized and transparent way that ensures mutual trust and a combined focus on achieving the strategic goals within the constraints of budgets and risk tolerance. Base relationships on open and transparent communication, a common language, and the willingness to take ownership and accountability for key decisions on both sides. Business and IT must work together to create successful enterprise outcomes in support of the enterprise objectives.

Purpose

Enable the right knowledge, skills and behaviors to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationship with business stakeholders.

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 • EG10 Staff skills, motivation and productivity • EG13 Product and business innovation	• AG05 Delivery of I&T services in line with business requirements • AG06 Agility to turn business requirements into operational solutions • 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	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	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
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	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
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	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

A. Component: Process	
Management Practice	**Example Metrics**
APO08.01 Understand business expectations. Understand current business issues, objectives and expectations for I&T. Ensure that requirements are understood, managed and communicated, and their status agreed and approved.	a. Number of identified current business issues b. Number of defined business requirements for I&T-enabled services

Activities	Capability Level
1. Identify business stakeholders, their interests and their areas of responsibilities.	2
2. Review current enterprise direction, issues, strategic objectives, and alignment with enterprise architecture.	
3. Understand the current business environment, process constraints or issues, geographical expansion or contraction, and industry/regulatory drivers.	
4. Maintain an awareness of business processes and associated activities. Understand demand patterns that relate to service volumes and use.	
5. Manage expectations by ensuring that business units understand priorities, dependencies, financial constraints and the need to schedule requests.	3
6. Clarify business expectations for I&T-enabled services and solutions. Ensure that requirements are defined with associated business acceptance criteria and metrics.	4
7. Confirm that there is agreement between IT and all business departments on expectations and how they will be measured. Ensure that this agreement is confirmed by all stakeholders.	

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

Management Practice	Example Metrics
APO08.02 Align I&T strategy with business expectations and identify opportunities for IT to enhance the business. Align I&T strategies with current business objectives and expectations to enable IT to be a value-add partner for the business and a governance component for enhanced enterprise performance.	a. Inclusion rate of technology opportunities in investment proposals b. Survey of business stakeholders regarding their level of technological awareness

Activities	Capability Level
1. Position IT as a partner to the business. Play a proactive role in identifying and communicating with key stakeholders on opportunities, risk and constraints. This includes current and emerging technologies, services and business process models.	3
2. Collaborate on major new initiatives with portfolio, program and project management. Ensure the involvement of the IT organization from the start of a new initiative by providing value-add advice and recommendations (e.g., for business case development, requirements definition, solution design) and by taking ownership for I&T work streams.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Strategy, 4.4 Demand management

Management Practice	Example Metrics
APO08.03 Manage the business relationship. Manage the relationship between the IT service organization and its business partners. Ensure that relationship roles and responsibilities are defined and assigned, and communication is facilitated.	a. Ratings of user and IT personnel satisfaction surveys b. Percent of relationship roles and responsibilities defined, assigned, and communicated

Activities	Capability Level
1. Assign a relationship manager as a single point of contact for each significant business unit. Ensure that a single counterpart is identified in the business organization and the counterpart has business understanding, sufficient technology awareness and the appropriate level of authority.	3
2. Manage the relationship in a formalized and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance.	
3. Define and communicate a complaints and escalation procedure to resolve any relationship issues.	
4. Ensure that key decisions are agreed and approved by relevant accountable stakeholders.	
5. Plan specific interactions and schedules based on mutually agreed objectives and common language (service and performance review meetings, review of new strategies or plans, etc.).	4

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	7.1 Business relationship management
ITIL V3, 2011	Service Strategy, 4.5 Business relationship management
Management Practice	**Example Metrics**
APO08.04 Coordinate and communicate. Work with all relevant stakeholders and coordinate the end-to-end delivery of I&T services and solutions provided to the business.	a. Time since last update of end-to-end communication plan to business b. Percent of business owner satisfaction with coordination of the end to end delivery of I&T services and solutions
Activities	**Capability Level**
1. Coordinate and communicate changes and transition activities such as project or change plans, schedules, release policies, release known errors, and training awareness.	2
2. Coordinate and communicate operational activities, roles and responsibilities, including the definition of request types, hierarchical escalation, major outages (planned and unplanned), and content and frequency of service reports.	
3. Take ownership of the response to the business for major events that may influence the relationship with the business. Provide direct support if required.	
4. Maintain an end-to-end communication plan that defines the content, frequency and recipients of service delivery information, including status of value delivered and any risk identified.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
APO08.05 Provide input to the continual improvement of services. Continually improve and evolve I&T-enabled services and service delivery to the enterprise to align with changing enterprise objectives and technology	a. Percent of alignment of I&T services with enterprise business requirements b. Percent of root causes identified and resolved for any issues
Activities	**Capability Level**
1. Perform customer and provider satisfaction analysis. Ensure that issues are addressed; report results and status.	4
2. Work together to identify, communicate and implement improvement initiatives.	5
3. Work with service management and process owners to ensure that I&T-enabled services and service management processes are continually improved and the root causes of any issues are identified and resolved.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

B. Component: Organizational Structures

Key Management Practice	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Business Process Owners	Relationship Manager	Head Architect	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO08.01 Understand business expectations.				A	R	R		R	R		R	R	R	R	R	R
APO08.02 Align I&T strategy with business expectations and identify opportunities for IT to enhance the business.				A	R	R	R	R	R	R	R	R	R			
APO08.03 Manage the business relationship.	R	R	R	A	R	R		R	R		R	R	R			
APO08.04 Coordinate and communicate.	R	R	R	A	R	R		R	R		R	R	R			
APO08.05 Provide input to the continual improvement of services.				A	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
APO08.01 Understand business expectations.	APO02.05	Strategic road map	Clarified and agreed business expectations	Internal
APO08.02 Align I&T strategy with business expectations and identify opportunities for IT to enhance the business.	APO09.01	Identified gaps in IT services to the business	Agreed next steps and action plans	Internal
	APO09.04	• Service level performance reports • Improvement action plans and remediations		
	APO11.03	Root causes of failure to deliver quality		
APO08.03 Manage the business relationship.	DSS02.02	Classified and prioritized incidents and service requests	Complaint and escalation status	Internal
	DSS02.06	• Closed service requests and incidents • User confirmation of satisfactory fulfilment or resolution	Agreed key decisions	Internal
	DSS02.07	• Incident status and trends report • Request fulfilment status and trends report		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO08.04 Coordinate and communicate.	**From**	**Description**	**Description**	**To**
	APO09.03	Service level agreements (SLAs)	Customer responses	Internal
	APO12.06	Risk impact communication	Communication packages	Internal
	BAI05.05	Operation and use plan	Communication plan	Internal
	BAI07.07	Supplemental support plan		
	BAI09.02	Communications of planned maintenance downtime		
	DSS03.04	Communication of knowledge learned		
APO08.05 Provide input to the continual improvement of services.	APO09.02	Service catalogs	Definition of potential improvement projects	APO02.02; BAI03.11
	APO11.02	• Customer requirements for quality management • Results of quality of service, including customer feedback	Satisfaction analyses	APO09.04
	APO11.03	Results of quality monitoring for solution and service delivery		
	APO11.04	Results of quality reviews and audits		
	BAI03.10	Maintenance plan		
	BAI05.05	Success measures and results		
	BAI07.07	Supplemental support plan		
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**
Relationship management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.4. Relationship Management
Relationship management	Skills Framework for the Information Age V6, 2015	RLMT

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Business—IT relationship management policy	Provides guidelines to establish and maintain relations between the business and IT. Fosters transparency, mutual trust and a common focus on achieving strategic goals within the context of budget and risk tolerance.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture based on mutual trust, transparent communication, open and understandable terms, a common language, ownership, and accountability. Good relationships must exist between the business and IT within the enterprise to achieve a shared goal.		

G. Component: Services, Infrastructure and Applications
• Collaboration platforms • Internal training and awareness building services

Domain: Align, Plan and Organize Management Objective: APO09 — Managed Service Agreements	Focus Area: COBIT Core Model

Description

Align I&T-enabled products and services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of I&T products and services, service levels and performance indicators.

Purpose

Ensure that I&T products, services and service levels meet current and future enterprise needs.

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
APO09.01 Identify I&T services. Analyze business requirements and the degree to which I&T-enabled services and service levels support business processes. Discuss and agree with the business on potential services and service levels. Compare potential service levels against the current service portfolio; identify new or changed services or service level options.	a. Number of business activities that are not supported by any I&T service b. Number of obsolete services identified

Activities	Capability Level
1. Assess current I&T services and service levels to identify gaps between existing services and the business activities they support. Identify areas for improvement of existing services and service level options.	2
2. Analyze, study and estimate future demand and confirm capacity of existing I&T-enabled services.	
3. Analyze business process activities to identify the need for new or redesigned I&T services.	3
4. Compare identified requirements to existing service components in the portfolio. If possible, package existing service components (I&T services, service level options and service packages) into new service packages to meet identified business requirements.	
5. Regularly review the portfolio of I&T services with portfolio management and business relationship management to identify obsolete services. Agree on retirement and propose change.	
6. Where possible, match demands to service packages and create standardized services to obtain overall efficiencies.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Strategy, 4.4 Demand management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO09.02 Catalog I&T-enabled services. Define and maintain one or more service catalogues for relevant target groups. Publish and maintain live I&T-enabled services in the service catalogs.	a. Percent of live I&T-enabled services and service packages offered in comparison to the portfolio b. Time since last service portfolio update
Activities	**Capability Level**
1. Publish in catalogues relevant live I&T-enabled services, service packages and service level options from the portfolio.	2
2. Continually ensure that the service components in the portfolio and the related service catalogues are complete and up to date.	3
3. Inform business relationship management of any updates to the service catalogues.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Design, 4.2 Service Catalogue Management
Management Practice	**Example Metrics**
APO09.03 Define and prepare service agreements. Define and prepare service agreements based on options in the service catalogues. Include internal operational agreements.	a. Number of business processes with undefined service agreements b. Percent of live IT services covered by service agreements
Activities	**Capability Level**
1. Analyze requirements for new or changed service agreements received from business relationship management to ensure that the requirements can be matched. Consider aspects such as service times, availability, performance, capacity, security, privacy, continuity, compliance and regulatory issues, usability, demand constraints, and data quality.	2
2. Draft customer service agreements based on the services, service packages and service level options in the relevant service catalogues.	
3. Finalize customer service agreements with business relationship management.	
4. Determine, agree on and document internal operational agreements to underpin the customer service agreements, if applicable.	3
5. Liaise with supplier management to ensure that appropriate commercial contracts with external service providers underpin the customer service agreements, if applicable.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SY2.1 Service Level Agreements
ISO/IEC 20000-1:2011(E)	4.5 Establish and improve the SMS; 6.1 Service level management
ITIL V3, 2011	Service Design, 4.3 Service Level Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-9)
Management Practice	**Example Metrics**
APO09.04 Monitor and report service levels. Monitor service levels, report on achievements and identify trends. Provide the appropriate management information to aid performance management.	a. Number and severity of service breaches b. Percent of customers satisfied that service delivery meets agreed levels c. Percent of service targets being met d. Percent of services being monitored to service levels
Activities	**Capability Level**
1. Establish and maintain measures to monitor and collect service level data.	4
2. Evaluate performance and provide regular and formal reporting of service agreement performance, including deviations from the agreed values. Distribute this report to business relationship management.	
3. Perform regular reviews to forecast and identify trends in service level performance. Incorporate quality management practices in the service monitoring.	
4. Provide the appropriate management information to aid performance management.	
5. Agree on action plans and remediations for any performance issues or negative trends.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	09.02 Control Third Party Service Delivery
ISO/IEC 20000-1:2011(E)	6.2 Service reporting

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO09.05 Review service agreements and contracts. Conduct periodic reviews of the service agreements and revise when needed.	a. Number of reviews of the service agreements performed b. Percent of service targets being met c. Percent of stakeholders satisfied with the quality of service agreements d. Number of service agreements revised, as needed

Activities	Capability Level
1. Regularly review service agreements according to the agreed terms to ensure that they are effective and up to date. When appropriate, take into account changes in requirements, I&T-enabled services, service packages or service level options.	3
2. When needed, revise the existing service agreement with the service provider. Agree on and update the internal operational agreements.	4

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**	**Enterprise Risk Committee**	**Business Process Owners**	**Head IT Operations**	**Head IT Administration**	**Service Manager**	**Information Security Manager**	**Privacy Officer**	**Legal Counsel**
APO09.01 Identify I&T services.	R	R	A		R			R			
APO09.02 Catalog I&T-enabled services.		R	A	R				R			
APO09.03 Define and prepare service agreements.		R	A			R	R	R	R	R	R
APO09.04 Monitor and report service levels.		R	A		R			R			R
APO09.05 Review service agreements and contracts.	R	A	R			R	R	R			

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	4.1.1 Management commitment

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
APO09.01 Identify I&T services.	**From**	**Description**	**Description**	**To**
			Identified gaps in I&T services to the business	APO01.10; APO02.02; APO05.02; APO08.02
			Definitions of standard services	EDM02.01
APO09.02 Catalog I&T-enabled services.	APO05.04	Updated portfolios of programs, services and assets	Service catalogs	APO08.05
	EDM04.01	Approved resources plan		
	EDM04.02	Communication of resourcing strategies		
APO09.03 Define and prepare service agreements.	APO11.02	Customer requirements for quality management	Service level agreements (SLAs)	APO05.02; APO08.04; DSS01.02; DSS02.01; DSS02.02; DSS04.01; DSS05.02; DSS05.03
	APO14.07	Data quality requirements	Operational level agreements (OLAs)	DSS01.02; DSS02.07; DSS04.03; DSS05.03
APO09.04 Monitor and report service levels.	APO05.03	Investment portfolio performance reports	Improvement action plans and remediations	APO02.02; APO08.02
	APO05.05	• Benefit results and related communications • Corrective actions to improve benefit realization	Service level performance reports	APO08.02; MEA01.03
	APO08.05	Satisfaction analyses		
	APO11.03	• Results of quality monitoring for solution and service delivery • Root causes of quality delivery failures		
	APO11.04	Results of quality reviews and audits		
	DSS02.02	Classified and prioritized incidents and service requests		
	DSS02.06	Closed service requests and incidents		
	DSS02.07	• Incident status and trends report • Status of request fulfilment and trends report		
	EDM04.03	Remedial actions to address resource management deviations		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO09.05 Review service agreements and contracts.	**From**	**Description**	**Description**	**To**
	APO11.02	Results of quality of service, including customer feedback	Updated SLAs	Internal
	APO11.04	Results of quality reviews and audits		
	BAI04.01	Evaluations against SLAs		
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 12. Project procurement management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Service level management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.2. Service Level Management
Service level management	Skills Framework for the Information Age V6, 2015	SLMO

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Service level agreement (SLA) policy	Describes general standards and criteria to inform specific requirements and terms for delivery of services, whether between entities within the enterprise or between the enterprise and a third party.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a contract between a service provider (internal or external) and the end user that defines expected level of service. Make sure this service level is based on output, specifically defining what the customer will receive in SMART objectives (specific, measurable, achievable, realistic and time-phased). Establish a culture in which service levels are respected. Discourage noncompliance through a penalty system.		

G. Component: Services, Infrastructure and Applications
• Contract management system • Service level monitoring tools

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO10 — Managed Vendors	Focus Area: COBIT Core Model

Description

Manage I&T-related products and services provided by all types of vendors to meet enterprise requirements. This includes the search for and selection of vendors, management of relationships, management of contracts, and reviewing and monitoring of vendor performance and vendor ecosystem (including upstream supply chain) for effectiveness and compliance.

Purpose

Optimize available I&T capabilities to support the I&T strategy and road map, minimize the risk associated with nonperforming or noncompliant vendors, and ensure competitive pricing.

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
APO10.01 Identify and evaluate vendor relationships and contracts. Continuously search for and identify vendors and categorize them into type, significance and criticality. Establish criteria to evaluate vendors and contracts. Review the overall portfolio of existing and alternative vendors and contracts.	a. Percent of defined evaluation criteria achieved for existing suppliers and contracts b. Percent of alternative suppliers providing equivalent services of existing supplier contracts

Activities	Capability Level
1. Continuously scan the enterprise landscape in search for new partners and vendors that can provide complementary capabilities and support the realization of the I&T strategy, road map and enterprise objectives.	3
2. Establish and maintain criteria relating to type, significance and criticality of vendors and vendor contracts, enabling a focus on preferred and important vendors.	
3. Identify, record and categorize existing vendors and contracts according to defined criteria to maintain a detailed register of preferred vendors that need to be managed carefully.	
4. Establish and maintain vendor and contract evaluation criteria to enable overall review and comparison of vendor performance in a consistent way.	4
5. Periodically evaluate and compare the performance of existing and alternative vendors to identify opportunities or a compelling need to reconsider current vendor contracts.	5

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

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO10.02 Select vendors. Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimized with input from potential suppliers.	a. Number of identified gaps between the selected supplier's offerings and the needs specified in the request for proposal (RFP) b. Percent of stakeholders satisfied with suppliers

Activities	Capability Level
1. Review all requests for information (RFIs) and requests for proposals (RFPs) to ensure that they clearly define requirements (e.g., enterprise requirements for security and privacy of information, operational business and I&T processing requirements, priorities for service delivery) and include a procedure to clarify requirements. The RFIs and RFPs should allow vendors sufficient time to prepare their proposals and should clearly define award criteria and the decision process.	2
2. Evaluate RFIs and RFPs in accordance with the approved evaluation process/criteria and maintain documentary evidence of the evaluations. Verify the references of candidate vendors.	
3. Select the vendor that best fits the RFP. Document and communicate the decision, and sign the contract.	
4. In the specific case of software acquisition, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include ownership and licensing of IP; maintenance; warranties; arbitration procedures; upgrade terms; and fit for purpose, including security, privacy, escrow and access rights.	3
5. In the specific case of acquisition of development resources, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include ownership and licensing of IP; fit for purpose, including development methodologies; testing; quality management processes, including required performance criteria; performance reviews; basis for payment; warranties; arbitration procedures; human resource management; and compliance with the enterprise's policies.	
6. Obtain legal advice on resource development acquisition agreements regarding ownership and licensing of IP.	
7. In the specific case of acquisition of infrastructure, facilities and related services, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include service levels, maintenance procedures, access controls, security, privacy, performance review, basis for payment and arbitration procedures.	

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

Management Practice	Example Metrics
APO10.03 Manage vendor relationships and contracts. Formalize and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.	a. Percent of third-party suppliers who have contracts defining control requirements b. Number of formal disputes with suppliers c. Number of supplier review meetings d. Percent of disputes resolved amicably in a reasonable time frame

Activities	Capability Level
1. Assign relationship owners for all vendors and make them accountable for the quality of service(s) provided.	3
2. Specify a formal communication and review process, including vendor interactions and schedules.	
3. Agree on, manage, maintain and renew formal contracts with the vendor. Ensure that contracts conform to enterprise standards and legal and regulatory requirements.	
4. Include provisions in contracts with key service vendors for review of the vendor site and internal practices and controls by management or independent third parties. Agree on independent audit and assurance controls of the operational environments of vendors providing outsourced services to confirm that agreed requirements are being adequately addressed.	
5. Use established procedures to deal with contract disputes. Whenever possible, first use effective relationships and communications to overcome service problems.	
6. Define and formalize roles and responsibilities for each service vendor. Where several vendors combine to provide a service, consider allocating a lead contractor role to one of the vendors to take responsibility for an overall contract.	
7. Evaluate the effectiveness of the relationship and identify necessary improvements.	4
8. Define, communicate and agree on ways to implement required improvements to the relationship.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	7.2 Supplier management
ITIL V3, 2011	Service Design, 4.8 Supplier Management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO10.04 Manage vendor risk. Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	a. Frequency of risk management sessions with supplier b. Number of risk-related events leading to service incidents c. Percent of risk-related incidents resolved acceptably (time and cost)

Activities	Capability Level
1. When preparing the contract, provide for potential service risk by clearly defining service requirements, including software escrow agreements, alternative vendors or standby agreements to mitigate possible vendor failure; security and protection of IP; privacy; and any legal or regulatory requirements.	3
2. Identify, monitor and, where appropriate, manage risk relating to the vendor's ability to deliver service efficiently, effectively, securely, confidentially, reliably and continually. Integrate critical internal IT management processes with those of the outsourced service providers, covering, for example, performance and capacity planning, change management, and configuration management.	4
3. Assess the larger ecosystem of the vendor and identify, monitor, and, where appropriate, manage risk related to the subcontractors and upstream vendors influencing the vendor's ability to deliver service efficiently, effectively, securely, reliably and continually.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	RM.MP Manage External Participation
ISF, The Standard of Good Practice for Information Security 2016	SC1.1 External Supplier Management Process
ISO/IEC 27002:2013/Cor.2:2015(E)	15. Supplier relationships
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	D.SC Supply Chain Risk Management

Management Practice	Example Metrics
APO10.05 Monitor vendor performance and compliance. Periodically review overall vendor performance, compliance to contract requirements and value for money. Address identified issues.	a. Number of service breaches to I&T-related services caused by suppliers b. Percent of suppliers meeting agreed requirements

Activities	Capability Level
1. Request independent reviews of vendor internal practices and controls, if necessary.	3
2. Define and document criteria to monitor vendor performance aligned with service level agreements. Ensure that the vendor regularly and transparently reports on agreed criteria.	4
3. Monitor and review service delivery to ensure that the vendor is providing an acceptable quality of service, meeting requirements and adhering to contract conditions.	
4. Review vendor performance and value for money. Ensure that the vendor is reliable and competitive, compared with alternative vendors and market conditions.	
5. Monitor and evaluate externally available information about the vendor and the vendor's supply chain.	
6. Record and assess review results periodically and discuss them with the vendor to identify needs and opportunities for improvement.	5

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

B. Component: Organizational Structures

Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Enterprise Risk Committee	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Privacy Officer	Legal Counsel
APO10.01 Identify and evaluate vendor relationships and contracts.		R	R	R	A				R				R
APO10.02 Select vendors.		R	R	R	A		R	R	R	R	R	R	
APO10.03 Manage vendor relationships and contracts.		R	R	R	A		R	R	R	R			R
APO10.04 Manage vendor risk.	R	R	R	R	A	R	R	R	R	R	R	R	
APO10.05 Monitor vendor performance and compliance.	R	R	R	R	A	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
APO10.01 Identify and evaluate vendor relationships and contracts.	Outside COBIT	Vendor contracts	Vendor catalog	BAI02.02
			Potential revisions to vendor contracts	Internal
			Vendor significance and evaluation criteria	Internal
APO10.02 Select vendors.	BAI02.02	High-level acquisition/ development plan	Vendor RFIs and RFPs	BAI02.01; BAI02.02
			RFI and RFP evaluations	BAI02.02
			Decision results of vendor evaluations	vendor evaluations BAI02.02; EDM04.01
APO10.03 Manage vendor relationships and contracts.	BAI03.04	Approved acquisition plan	Results and suggested improvements	Internal
			Communication and review process	Internal
			Vendor roles and responsibilities	Internal
APO10.04 Manage vendor risk.	APO12.04	• Risk analysis and risk profile reports for stakeholders • Results of third-party risk assessments	Identified vendor delivery risk	APO12.01; APO12.03; BAI01.01; BAI11.01
			Identified contract requirements to minimize risk	Internal
APO10.05 Monitor vendor performance and compliance.			Vendor compliance monitoring criteria	Internal
			Vendor compliance monitoring review results	MEA01.03

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*	
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**
Contract management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.8. Contract Management
Contract management	Skills Framework for the Information Age V6, 2015	ITCM
Purchasing	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.4. Purchasing
Sourcing	Skills Framework for the Information Age V6, 2015	SORC

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
IT procurement policy	Outlines principles and procedures for procuring IT hardware, software and hosting solutions. Details standards for operating systems, computer networks, hardware specifications, etc. Provides guidelines for contract management (e.g., terms and conditions, monitoring of contracts).		
Third-party IT service delivery management policy	Sets guidelines for managing risk related to third-party services. Establishes framework of expectations for behavior and enumerates security precautions required of third-party service providers in managing risk related to provided services.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Build and manage an ecosystem of vendors that can assist the organization in its digital transformation and innovation. Continuously scan the landscape in search of new and effective partners.		
Management sets the tone and exemplifies correct behaviors when communicating with vendors to agree on and implement required improvements. Ensure that contracts conform to enterprise standards, and legal and regulatory requirements.		

G. Component: Services, Infrastructure and Applications
• Contract management system • Third-party assurance services

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO11 — Managed Quality	Focus Area: COBIT Core Model

Description

Define and communicate quality requirements in all processes, procedures and related enterprise outcomes. Enable controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts.

Purpose

Ensure consistent delivery of technology solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.

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 • EG12 Managed digital transformation programs	• AG09 Delivering programs on time, on budget and meeting requirements and quality standards • 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	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
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		
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**
APO11.01 Establish a quality management system (QMS). Establish and maintain a quality management system (QMS) that provides a standard, formal and continuous approach to quality management of information. The QMS should enable technology and business processes to align with business requirements and enterprise quality management.	a. Percent of effectiveness of quality management reviews b. Percent of key stakeholder satisfaction with quality management review program
Activities	**Capability Level**
1. Ensure that the I&T control framework and the business and IT processes include a standard, formal and continuous approach to quality management that is aligned with enterprise requirements. Within the I&T control framework and the business and IT processes, identify quality requirements and criteria (e.g., based on legal requirements and requirements from customers).	3
2. Define roles, tasks, decision rights and responsibilities for quality management in the organizational structure.	
3. Obtain input from management and external and internal stakeholders on the definition of quality requirements and quality management criteria.	
4. Regularly monitor and review the QMS against agreed acceptance criteria. Include feedback from customers, users and management.	4
5. Respond to discrepancies in review results to continuously improve the QMS.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8.1 Plan quality management
Management Practice	**Example Metrics**
APO11.02 Focus quality management on customers. Focus quality management on customers by determining their requirements and ensuring integration in quality management practices.	a. Percent of customer satisfaction b. Percent of customer requirements and expectations communicated throughout the business and IT organization
Activities	**Capability Level**
1. Focus quality management on customers by determining internal and external customer requirements and ensuring alignment of the I&T standards and practices. Define and communicate roles and responsibilities concerning conflict resolution between the user/customer and the IT organization.	3
2. Manage the business needs and expectations for each business process, IT operational service and new solutions. Maintain their quality acceptance criteria.	
3. Communicate customer requirements and expectations throughout the business and IT organization.	
4. Periodically obtain customer views on business process and service provisioning and IT solution delivery. Determine the impact on I&T standards and practices and ensure that customer expectations are met and actioned.	4
5. Capture quality acceptance criteria for inclusion in SLAs.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions. Identify and maintain standards, procedures and practices for key processes to guide the enterprise in meeting the intent of the agreed quality management standards (QMS). This activity should align with I&T control framework requirements. Consider certification for key processes, organizational units, products or services.	a. Number of processes with defined quality requirements b. Number of defects uncovered prior to production c. Number of services with a formal quality management plan d. Number of SLAs that include quality acceptance criteria

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Define the quality management standards, practices and procedures in line with the I&T control framework's requirements and enterprise quality management criteria and policies.	2
2. Integrate the required quality management practices in key processes and solutions across the organization.	3
3. Consider the benefits and costs of quality certifications.	
4. Effectively communicate the quality management approach (e.g., through regular, formal quality training programs).	
5. Record and monitor quality data. Use industry good practices for reference when improving and tailoring the enterprise's quality practices.	4
6. Regularly review the continued relevance, efficiency and effectiveness of specific quality management processes. Monitor the achievement of quality objectives.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8.2 Manage quality
Management Practice	**Example Metrics**
APO11.04 Perform quality monitoring, control and reviews. Monitor the quality of processes and services on an ongoing basis, in line with quality management standards. Define, plan and implement measurements to monitor customer satisfaction with quality as well as the value provided by the quality management system (QMS). The information gathered should be used by the process owner to improve quality.	a. Percent of solutions and services delivered with formal certification b. Average stakeholder satisfaction rating of solutions and services c. Number of processes with a formal quality assessment report d. Percent of projects reviewed that meet target quality goals and objectives e. Number, robustness and timeliness of risk analyses
Activities	**Capability Level**
1. Prepare and conduct quality reviews for key organizational processes and solutions.	3
2. For these key organizational processes and solutions, monitor goal-driven quality metrics aligned to overall quality objectives.	4
3. Ensure that management and process owners regularly review quality management performance against defined quality metrics.	
4. Analyze overall quality management performance results.	
5. Report the quality management performance review results and initiate improvements where appropriate.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8.3 Control quality
Management Practice	**Example Metrics**
APO11.05 Maintain continuous improvement. Maintain and regularly communicate an overall quality plan that promotes continuous improvement. The plan should define the need for, and benefits of, continuous improvement. Collect and analyze data about the quality management system (QMS) and improve its effectiveness. Correct nonconformities to prevent recurrence.	a. Number of root cause analyses performed b. Percent of on-time and complete services and products
Activities	**Capability Level**
1. Establish a platform to share good practices and capture information on defects and mistakes to enable learning from them.	2
2. Identify examples of excellent quality delivery processes that can benefit other services or projects. Share these with the service and project delivery teams to encourage improvement.	3
3. Identify recurring examples of quality defects. Determine their root cause, evaluate their impact and result, and agree on improvement actions with the service and/or project delivery teams.	
4. Provide employees with training in the methods and tools of continual improvement.	
5. Benchmark the results of the quality reviews against internal historical data, industry guidelines, standards and data from similar types of enterprises.	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	DE.DP Detection Processes

B. Component: Organizational Structures

Key Management Practice	Chief Operating Officer	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Business Process Owners	Portfolio Manager	Program Manager	Project Manager	Project Management Office	Data Management Function	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager
APO11.01 Establish a quality management system (QMS).	A		R		R											R	R		
APO11.02 Focus quality management on customers.			A		R		R										R		
APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions.			A	R	R		R	R	R	R	R	R	R	R	R	R	R	R	R
APO11.04 Perform quality monitoring, control and reviews.		R	A		R	R	R										R		
APO11.05 Maintain continuous improvement.			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
APO11.01 Establish a quality management system (QMS).	Outside COBIT	Enterprisewide quality system	Quality management system (QMS) roles, responsibilities and decision rights	APO01.05; DSS06.03
			Quality management plans	APO14.04; APO14.06; BAI01.07; BAI11.05
			Results of QMS effectiveness reviews	BAI03.06
APO11.02 Focus quality management on customers.	Outside COBIT	Business and customer quality requirements	Customer requirements for quality management	APO08.05; APO09.03; BAI01.07; BAI11.06
			Results of quality of service, including customer feedback	APO08.05; APO09.05; BAI05.01; BAI07.07
			Acceptance criteria	BAI02.01; BAI02.02

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions.	BAI02.04	Approved quality reviews	Quality management standards	All APO; All BAI; All DSS; All MEA
	Outside COBIT	• Available quality certifications • Industry good practices	Root causes of quality delivery failures	APO08.02; APO09.04; BAI07.08; MEA02.04; MEA04.04
			Results of quality monitoring	APO08.05; APO09.04; BAI07.08
APO11.04 Perform quality monitoring, control and reviews.	BAI03.06	• Quality assurance plan • Quality review results, exceptions and corrections	Process quality of service goals and metrics	All APO; All BAI; All DSS; All MEA
	DSS02.07	• Incident status and trends report • Status of request fulfilment and trends report	Results of quality reviews and audits	APO08.05; APO09.04; APO09.05; BAI07.08
APO11.05 Maintain continuous improvement.			Quality review benchmark results	All APO; All BAI; All DSS; All MEA
			Examples of good practice to be shared	All APO; All BAI; All DSS; All MEA
			Communications on continual improvement and best practices	All APO; All BAI; All DSS; All MEA

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 8. Project quality management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
ICT quality strategy development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.2. ICT Quality Strategy Development
Quality assurance	Skills Framework for the Information Age V6, 2015	QUAS
Quality management	Skills Framework for the Information Age V6, 2015	QUMG
Quality standards	Skills Framework for the Information Age V6, 2015	QUST

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Quality management policy	Captures management's vision of enterprise quality objectives, acceptable level of quality, and duties of specific teams and entities to ensure quality.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote a culture of quality and continual improvement. Maintain and regularly communicate the need for, and benefits of, quality and continuous improvement.		

G. Component: Services, Infrastructure and Applications
• QMS • Third-party quality assurance services

Domain: Align, Plan and Organize Management Objective: APO12 — Managed Risk	Focus Area: COBIT Core Model

Description

Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.

Purpose

Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.

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
APO12.01 Collect data. Identify and collect relevant data to enable effective I&T-related risk identification, analysis and reporting.	a. Number of loss events with key characteristics captured in repositories b. Percent of audits, events and trends captured in repositories c. Percent of critical systems with known issues

Activities	Capability Level
1. Establish and maintain a method for the collection, classification and analysis of I&T risk-related data.	2
2. Record relevant and significant I&T risk-related data on the enterprise's internal and external operating environment.	
3. Adopt or define a risk taxonomy for consistent definitions of risk scenarios and impact and likelihood categories.	3
4. Record data on risk events that have caused or may cause business impacts as per the impact categories defined in the risk taxonomy. Capture relevant data from related issues, incidents, problems and investigations.	
5. Survey and analyze the historical I&T risk data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.	4
6. For similar classes of events, organize the collected data and highlight contributing factors. Determine common contributing factors across multiple events.	
7. Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.	
8. Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an understanding of the associated internal and external risk factors.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes - Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 10
ISO/IEC 27005:2011(E)	8.2 Risk identification; 12. Information security risk monitoring and review
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO12.02 Analyze risk. Develop a substantiated view on actual I&T risk, in support of risk decisions.	a. Number of identified I&T risk scenarios b. Time since last update of I&T risk scenarios

Activities	Capability Level
1. Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of assets.	3
2. Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop expectations for specific control activities and capabilities to detect.	
3. Estimate the frequency (or likelihood) and magnitude of loss or gain associated with I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.	
4. Compare current risk (I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or elevated risk.	
5. Propose risk responses for risk exceeding risk appetite and tolerance levels.	
6. Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.	
7. Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise requirements and verify that estimations were properly calibrated and scrutinized for bias.	4
8. Analyze cost/benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 11
ISF, The Standard of Good Practice for Information Security 2016	IR2.1 Risk Assessment Scope; IR2.2 Business Impact Assessment
ISO/IEC 27001:2013/Cor.2:2015(E)	8.2 Information security risk assessment
ISO/IEC 27005:2011(E)	8.3 Risk analysis
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.RA Risk Assessment
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 3)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-3)

Management Practice	Example Metrics
APO12.03 Maintain a risk profile. Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	a. Completeness of attributes and values in the risk profile b. Percent of key business processes included in the risk profile

Activities	Capability Level
1. Inventory business processes and document their dependency on I&T service management processes and IT infrastructure resources. Identify supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers.	2
2. Determine and agree on which I&T services and IT infrastructure resources are essential to sustain the operation of business processes. Analyze dependencies and identify weak links.	
3. Aggregate current risk scenarios by category, business line and functional area.	
4. Regularly capture all risk profile information and consolidate it into an aggregated risk profile.	3
5. Capture information on the status of the risk action plan for inclusion in the I&T risk profile of the enterprise.	
6. Based on all risk profile data, define a set of risk indicators that allow the quick identification and monitoring of current risk and risk trends.	4
7. Capture information on I&T risk events that have materialized for inclusion in the IT risk profile of the enterprise.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RS.DT Define Organizational Risk Tolerance
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 12
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-7)
Management Practice	**Example Metrics**
APO12.04 Articulate risk. Communicate information on the current state of I&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	a. Level of stakeholder satisfaction with provided risk reporting b. Completeness of risk profile reporting (including information in line with stakeholder requirements) c. Use of risk reporting in management decision making
Activities	**Capability Level**
1. Report the results of risk analysis to all affected stakeholders in terms and formats useful to support enterprise decisions. Whenever possible, include probabilities and ranges of loss or gain along with confidence levels, to enable management to balance risk-return.	3
2. Provide decision makers with an understanding of worst-case and most-probable scenarios, I&T-related loss exposures and significant reputation, legal and regulatory considerations, or any other impact category as per the risk taxonomy.	
3. Report the current risk profile to all stakeholders. Include information on the effectiveness of the risk management process, control effectiveness, gaps, inconsistencies, redundancies, remediation status and their impacts on the risk profile.	
4. On a periodic basis, for areas with relative risk and risk capacity parity, identify I&T-related opportunities that would allow the acceptance of greater risk and enhanced growth and return.	
5. Review the results of objective third-party assessments and internal audit and quality assurance reviews. Include them in the risk profile. Review identified gaps and I&T-related loss exposures to determine the need for additional risk analysis.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RS.CR Determine Critical Infrastructure Requirements
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting—Principle 19
ISO/IEC 27005:2011(E)	11. Information security risk communication and consultation
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.RM Risk Management Strategy
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-32)
Management Practice	**Example Metrics**
APO12.05 Define a risk management action portfolio. Manage opportunities to reduce risk to an acceptable level as a portfolio.	a. Number of significant incidents not identified and included in the risk management portfolio b. Percent of risk management project proposals rejected due to lack of consideration of other related risk
Activities	**Capability Level**
1. Maintain an inventory of control activities that are in place to mitigate risk and that enable risk to be taken in line with the risk appetite and tolerance. Classify control activities and map them to specific I&T risk scenarios and aggregations of I&T risk scenarios.	2
2. Determine whether each organizational entity monitors risk and accepts accountability for operating within its individual and portfolio tolerance levels.	3
3. Define a balanced set of project proposals designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering costs, benefits, effect on current risk profile and regulations.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 14
HITRUST CSF version 9, September 2017	03.01 Risk Management Program

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO12.06 Respond to risk. Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.	a. Number of measures not reducing residual risk b. Percent of I&T risk action plans executed as designed

Activities	Capability Level
1. Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a significant operational or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.	3
2. Apply the appropriate response plan to minimize the impact when risk incidents occur.	
3. Categorize incidents and compare I&T-related loss exposures against risk tolerance thresholds. Communicate business impacts to decision makers as part of reporting and update the risk profile.	4
4. Examine past adverse events/losses and missed opportunities and determine root causes.	
5. Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers. Ensure that the cause, response requirements and process improvement are included in risk governance processes.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 13
ISF, The Standard of Good Practice for Information Security 2016	IR2.9 Risk Treatment
ISO/IEC 27001:2013/Cor.2:2015(E)	6.1 Action to address risk and opportunities
ISO/IEC 27005:2011(E)	9. Information security risk treatment
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 4)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-9, PM-31)

B. Component: Organizational Structures

Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Data Management Function	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
APO12.02 Analyze risk.	A	R			R		R										
APO12.03 Maintain a risk profile.	A	R			R		R										
APO12.04 Articulate risk.	A	R			R		R										
APO12.05 Define a risk management action portfolio.	A	R			R		R										
APO12.06 Respond to risk.	R	A	R	R		R	R	R		R	R	R	R	R	R	R	R

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 1); Appendix A: Roles and Responsibilities

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
APO12.01 Collect data.	**From**	**Description**	**Description**	**To**
	APO02.02	Gaps and risk related to current capabilities	Emerging risk issues and factors	APO01.01; APO02.02; EDM03.01
	APO02.05	Risk assessment initiatives	Data on risk events and contributing factors	Internal
	APO10.04	Identified vendor delivery risk	Data on the operating environment relating to risk	Internal
	DSS02.07	Incident status and trends report		
	EDM03.01	Evaluation of risk management activities		
	EDM03.02	• Risk management policies • Key objectives to be monitored for risk management • Approved process for measuring risk management		
APO12.02 Analyze risk.	DSS04.02	Business impact analyses (BIAs)	Risk analysis results	APO01.01; APO02.02; EDM03.03; BAI01.08; BAI11.06
	DSS05.01	Evaluations of potential threats	I&T risk scenarios	Internal
	Outside COBIT	Threat advisories	Scope of risk analysis efforts	Internal
APO12.03 Maintain a risk profile.	APO10.04	Identified vendor delivery risk	Aggregated risk profile, including status of risk management actions	APO02.02; EDM03.02
	DSS05.01	Evaluations of potential threats	Documented risk scenarios by line of business and function	Internal
	EDM03.01	• Risk appetite guidance • Approved risk tolerance levels		
APO12.04 Articulate risk.			Risk analysis and risk profile reports for stakeholders	APO10.04; EDM03.03; EDM05.02; MEA04.05
			Results of third-party risk assessments	APO10.04; EDM03.03; MEA02.01
			Opportunities for acceptance of greater risk	EDM03.03

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
APO12.05 Define a risk management action portfolio.	**From**	**Description**	**Description**	**To**
			Project proposals for reducing risk	APO02.02; APO13.02
APO12.06 Respond to risk.	EDM03.03	Remedial actions to address risk management deviations	Risk impact communication	APO01.02; APO08.04; DSS04.02
			Risk-related root causes	DSS02.03; DSS03.01; DSS03.02; DSS03.03; DSS03.05; DSS04.02; MEA02.04; MEA04.04; MEA04.06
			Risk-related incident response plans	DSS02.05

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting—Principle 20
SF, The Standard of Good Practice for Information Security 2016	IR1.3 Information Risk Assessment—Supporting Material
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.6 Authorization (Task 3, 4): Inputs and Outputs
PMBOK Guide Sixth Edition, 2017	Part 1: 11. Project risk management: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business risk management	Skills Framework for the Information Age V6, 2015	BURM
Information assurance	Skills Framework for the Information Age V6, 2015	INAS
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**
Enterprise risk policy	Defines governance and management of enterprise risk at strategic, tactical and operational levels, pursuant to business objectives. Translates enterprise governance into risk governance principles and policy and elaborates risk management activities.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-1)
Fraud risk policy	Informs protection of enterprise brand, reputation and assets in the event of loss or damage resulting from fraud or misconduct. Guides employees in reporting suspicious activity and handling sensitive information and evidence. Encourages antifraud culture and cultivates awareness of risk.	National Institute of Standards and Technology Special Publication 800- 37, Revision 2 (Draft), May 2018	

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
To support a transparent and participatory risk culture, senior management should set direction and demonstrate visible and genuine support for incorporation of risk practices throughout the enterprise. Management should encourage open communication and business ownership for I&T-related business risk. Desirable behaviors include aligning policies to the defined risk appetite, reporting risk trends to senior management and risk governing bodies, rewarding effective risk management, and proactively monitoring risk and progress on the risk action plan.	ISF, The Standard of Good Practice for Information Security 2016	IR1.2 Information Risk Assessment

G. Component: Services, Infrastructure and Applications
• Crisis management services • Governance, risk and compliance (GRC) tools • Risk analysis tools • Risk intelligence services

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO13 — Managed Security	Focus Area: COBIT Core Model

Description

Define, operate and monitor an information security management system.

Purpose

Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.

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

Enterprise Goals	Alignment Goals
• EG02 Managed business risk • EG06 Business service continuity and availability	AG07 Security of information, processing infrastructure and applications, and privacy

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG02	a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG07	a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment
EG06	a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets		

A. Component: Process

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

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

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	0.01 Information Security Management program
ISO/IEC 20000-1:2011(E)	6.6 Information security management
ITIL V3, 2011	Service Design, 4.7 Information Security Management
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 1); 3.4 Implementation (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-2)
Management Practice	**Example Metrics**
APO13.02 Define and manage an information security and privacy risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases, implemented as an integral part of services and solutions development, and operated as an integral part of business operation.	a. Percentage of successful security risk scenario simulations b. Number of employees who have successfully completed information security awareness training

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

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	
Management Practice	**Example Metrics**
APO13.03 Monitor and review the information security management system (ISMS). Maintain and regularly communicate the need for, and benefits of, continuous improvement in information security. Collect and analyze data about the information security management system (ISMS), and improve its effectiveness. Correct nonconformities to prevent recurrence.	a. Frequency of scheduled security reviews b. Number of findings in regularly scheduled security reviews c. Level of stakeholder satisfaction with the security plan d. Number of security-related incidents caused by failure to adhere to the security plan

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

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

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

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
APO13.01 Establish and maintain an information security management system (ISMS).	Outside COBIT	Enterprise security approach	ISMS scope statement	APO01.05; DSS06.03
			ISMS policy	Internal
APO13.02 Define and manage an information security risk treatment plan.	APO02.04	Gaps and changes required to realize target capability	Information security risk treatment plan	All APO; All BAI; All DSS; All MEA; ALL EDM
	APO03.02	Baseline domain descriptions and architecture definition	Information security business cases	APO05.02
	APO12.05	Project proposals for reducing risk		

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

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

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

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

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

Domain: Align, Plan and Organize Management Objective: APO14 — Managed Data	Focus Area: COBIT Core Model

Description

Achieve and sustain effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving.

Purpose

Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.

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	AG10 Quality of I&T management 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	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		

A. Component: Process

Management Practice	Example Metrics
APO14.01 Define and communicate the organization's data management strategy and roles and responsibilities. Define how to manage and improve the organization's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	a. Number of data management breaches in comparison to the defined strategy b. Percent of roles and responsibilities identified to support the governance of data management and the interaction between governance and the data management function

Activities	Capability Level
1. Establish a data management function with responsibility for managing activities that support data management objectives.	2
2. Specify roles and responsibilities to support the management of data and the interaction between governance and the data management function.	
3. Ensure that business and technology collaboratively develop the organization's data management strategy. Make sure that data management objectives, priorities and scope reflect enterprise objectives, are consistent with data management policies and regulation, and are approved by all stakeholders.	3
4. Communicate data management objectives, priorities and scope and adjust them as needed, based upon feedback.	
5. Use metrics to assess and monitor the achievement of objectives for data management.	4
6. Monitor the sequence plan for implementation of the data management strategy. Update it as needed, based on progress reviews.	
7. Use statistical and other quantitative techniques to evaluate the effectiveness of strategic data management objectives in achieving business objectives. Make modifications as needed, based on metrics.	
8. Ensure that the organization researches innovative business processes and emerging regulatory requirements to ensure that the data management program is compatible with future business needs.	5
9. Make contributions to industry best practices for data management strategy development and implementation.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Management Strategy - Data Management Strategy; Data Governance—Governance Management
ITIL V3, 2011	Service Design, 5.2 Management of Data and Information
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 13: Data Protection
Management Practice	**Example Metrics**
APO14.02 Define and maintain a consistent business glossary. Create, approve, update and promote consistent business terms and definitions to foster shared data usage across the organization.	a. Level of acceptance and frequency of use of business glossary terms throughout the entire organization b. Number of synonyms for defined business glossary terminology that are used in new development efforts c. Level of granularity of defined business glossary terms

Activities	Capability Level
1. Ensure that standard business terms are readily available and communicated to relevant stakeholders.	2
2. Ensure that each business term added to the business glossary has a unique name and unique definition.	
3. Use standard industry business terms and definitions, as appropriate, in the business glossary.	
4. Establish, document and follow a process to define, manage, use and maintain the business glossary. For example, new initiatives should apply standard business terms as part of the data requirements definition process to ensure consistency of language. This will help achieve comparability of the content and facilitate data sharing across the organization.	3
5. Ensure that new development, data integration and data consolidation efforts apply standard business terms as part of the data requirements definition process.	
6. Integrate the business glossary into the organization's metadata repository, with appropriate access permissions.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Data Governance - Business Glossary
ISF, The Standard of Good Practice for Information Security 2016	IM1.1 Information Classification and Handling
Management Practice	**Example Metrics**
APO14.03 Establish the processes and infrastructure for metadata management. Establish the processes and infrastructure for specifying and extending metadata about the organization's data assets, fostering and supporting data sharing, ensuring compliant use of data, improving responsiveness to business changes and reducing data-related risk.	a. Number of identified inaccuracies in metadata b. Percent of metadata containing measures and metrics to evaluate the accuracy and adoption of metadata

Activities	Capability Level
1. Establish and follow a metadata management process.	2
2. Ensure that metadata documentation captures data interdependencies.	
3. Establish and follow metadata categories, properties and standards.	
4. Develop and use metadata to perform impact analysis on potential data changes.	3
5. Populate the organization's metadata repository with additional categories and classifications of metadata according to a phased implementation plan. Link it to architecture layers.	
6. Validate metadata and any changes to metadata against the existing architecture.	
7. Ensure that the organization has developed an integrated metamodel deployed across all platforms.	
8. Ensure that metadata types and data definitions support consistent import, subscription and consumption practices.	
9. Use measures and metrics to evaluate the accuracy and adoption of metadata.	4
10. Evaluate planned data changes for impact on the metadata repository. Continuously improve metadata capture, change and refinement processes.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Data Governance—Metadata Management
ISO/IEC 27002:2013/Cor.2:2015(E)	8.2 Information classification

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO14.04 Define a data quality strategy. Define an integrated, organizationwide strategy to achieve and maintain the level of data quality (such as complexity, integrity, accuracy, completeness, validity, traceability and timeliness) required to support the business goals and objectives.	a. Number of data quality improvement efforts identified and recorded in a sequence plan b. Percent of stakeholders satisfied with the quality of data

Activities	Capability Level
1. Define a data quality strategy in collaboration with business and technology stakeholders, approved by executive management, and managed. The strategy should facilitate moving from the current to the target state. It should also explicitly align with business objectives and the organization's data management strategy.	3
2. Ensure that the data quality strategy is followed across the organization and is accompanied by corresponding policies, processes and guidelines.	
3. Anchor the policies, processes and governance contained in the data quality strategy across the data life cycle. Mandate corresponding processes in the system development life cycle methodology.	
4. Develop, monitor and maintain a sequence plan for data quality improvement efforts across the organization.	
5. To evaluate progress, monitor plans to meet the goals and objectives of the data quality strategy.	4
6. Systematically collect stakeholder reports of data quality issues. Include their expectations for improving data quality in the data quality strategy. Measure and monitor them.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	DP.DR Safeguard Data at Rest; DP.DT Safeguard Data in Transit; DP.IP Integrity and Data Leak Prevention
CMMI Data Management Maturity Model, 2014	Data Quality - Data Quality Strategy

Management Practice	Example Metrics
APO14.05 Establish data profiling methodologies, processes and tools. Implement standardized data profiling methodologies, processes, practices, tools and templates that can be applied across multiple data repositories and data stores.	a. Number of defined and implemented data templates and their usage percentage b. Number of shared data sets with a defined data profile

Activities	Capability Level
1. Define and standardize data profiling methodologies, processes, practices, tools and results templates. Ensure that profiling processes are reusable and leveraged across multiple data stores and shared data repositories.	3
2. Engage data management to identify core shared data sets that are regularly profiled and monitored.	4
3. In data profiling efforts, include evaluation of the conformity of data content with its approved metadata and standards.	
4. During a data profiling activity, compare actual issues to the statistically predicted issues, based on historical profiling results.	
5. Ensure that results are centrally stored, systematically monitored and analyzed with respect to statistics and metrics. Provide the resulting insight to data quality improvements over time.	
6. Create real-time or near real-time automated profiling reports for all critical data feeds and repositories.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Data Quality—Data Profiling
National Institute of Standards and Technology Special Publication 800-53, Revision 5, August 2017	3.20 System and information integrity (SI-1)

Management Practice	Example Metrics
APO14.06 Ensure a data quality assessment approach. Provide a systematic approach to measure and evaluate data quality according to processes and techniques, and against data quality rules.	a. Number of identified issues in data quality assessment results b. Number of data quality assessment results that include recommendations for remediation

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Periodically conduct data quality assessments, according to an approved frequency per the data quality assessment policy. Ensure that data governance determines the key set of attributes by subject area for data quality assessments.	4
2. Include recommendations for remediation, with supporting rationale, in data quality assessment results.	
3. Assess data quality, using established thresholds and targets for each selected quality dimension.	
4. Systematically generate data quality measurement reports, based on criticality of attributes and data volatility.	
5. Continuously review and improve data quality assessment and reporting processes.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Quality—Data Quality Assessment
Management Practice	**Example Metrics**
APO14.07 Define the data cleansing approach. Define the mechanisms, rules, processes, and methods to validate and correct data according to predefined business rules.	a. Percent of data cleansed correctly b. Percent of SLAs that include data quality criteria and hold data providers accountable for cleansed data
Activities	**Capability Level**
1. Establish and maintain a data cleansing policy.	2
2. Maintain data change history through cleansing activities.	3
3. Establish methods for correcting the data and define those methods within a plan. Methods may include multiple repository comparison, verification against a valid source, logic checks, referential integrity or range tolerance.	4
4. In service level agreements, include data quality criteria to hold data providers accountable for cleansed data.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Quality—Data Cleansing
Management Practice	**Example Metrics**
APO14.08 Manage the life cycle of data assets. Ensure that the organization understands, maps, inventories and controls its data flows through business processes over the data life cycle, from creation or acquisition to retirement.	a. Number of requirements from data consumers that cannot be mapped to a data source b. Number of shared data sets c. Time since last compliance check regarding mappings of business processes to data
Activities	**Capability Level**
1. Map and align the requirements of data consumers and producers.	2
2. Define business process-to-data mappings. Maintain them and periodically review them for compliance.	3
3. Follow a defined process for collaborative agreements with respect to shared data and data usage within business processes.	
4. Implement data flows and full data-to-process life cycle maps for shared data for each major business process at the organizational level.	
5. Ensure that changes to shared data sets or target data sets for a specific business purpose are managed by data governance structures, with relevant stakeholder engagement.	
6. Use metrics to expand approved shared data reuse and eliminate process redundancy.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Operations—Data Lifecycle Management

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO14.09 Support data archiving and retention. Ensure that data maintenance satisfies organizational and regulatory requirements for availability of historical data. Ensure that legal and regulatory requirements for data archiving and retention are met.	a. Percent of unsuccessful attempts to transfer data to archive b. Percent of data maintenance that meets organizational and regulatory requirements for historical data availability and legal and regulatory requirements for data archiving and retention

Activities	Capability Level
1. Ensure that policies mandate management of data history, including retention, destruction and audit trail requirements.	2
2. Ensure the existence of a defined method that guarantees accessibility to the historical data necessary to support business needs.	
3. Use policy and processes to control access, transmittal and modifications to historical and archived data.	
4. Ensure that the organization has a prescribed data warehouse repository that provides access to historical data for meeting analytics needs supporting business processes.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Historical Data, Retention and Archiving

Management Practice	Example Metrics
APO14.10 Manage data backup and restore arrangements. Manage availability of critical data to ensure operational continuity.	a. Percent of unsuccessful attempts to back up data b. Percent of successful attempts to restore backup data

Activities	Capability Level
1. Define a schedule to ensure correct backup of all critical data.	2
2. Define requirements for on-site and off-site storage of backup data, taking into account volume, capacity and retention period, in alignment with the business requirements.	
3. Establish a testing schedule for backup data. Ensure that the data can be restored correctly without drastically impacting business.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 10: Data Recovery Capability

B. Component: Organizational Structures

Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Digital Officer	Enterprise Risk Committee	Chief Information Security Officer	Data Management Function	Legal Counsel
APO14.01 Define and communicate the organization's data management strategy and roles and responsibilities.	R	A	R		R	R	
APO14.02 Define and maintain a consistent business glossary.	R	A	R		R	R	
APO14.03 Establish the processes and infrastructure for metadata management.	R	A	R		R	R	
APO14.04 Define a data quality strategy.	R	A	R		R	R	
APO14.05 Establish data profiling methodologies, processes and tools.	R	A	R		R	R	
APO14.06 Ensure a data quality assessment approach.	R	A	R		R	R	
APO14.07 Define the data cleansing approach.	R	A	R		R	R	
APO14.08 Manage the life cycle of data assets.	R	A	R	R	R	R	R
APO14.09 Support data archiving and retention.	R	A	R	R	R	R	R
APO14.10 Manage data backup and restore arrangements.	R	A	R		R	R	R

B. Component: Organizational Structures *(cont.)*	
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**
APO14.01 Define and communicate the organization's data management strategy and roles and responsibilities.	APO01.06	Data classification guidelines	Data management strategy	APO03.02; APO14.10
	APO07.03	Skills and competencies matrix	Agreed roles and responsibilities for data management and data governance	Internal
	Outside COBIT	• Enterprise strategy • Data management policies and regulation	External publications and presentations about best practices at industry conferences	Internal
			Implementation plan for data management strategy	Internal
APO14.02 Define and maintain a consistent business glossary.			Business glossary	APO14.03; BAI02.01
APO14.03 Establish the processes and infrastructure for metadata management.	APO03.02	Information architecture model	Metadata documentation	APO03.02
	APO14.02	Business glossary		
APO14.04 Define a data quality strategy.	APO01.06	Data integrity procedures	Data quality strategy	APO14.05; APO14.06; APO14.07
	APO01.07	Data security and control guidelines	Data quality issue reports	Internal
	APO11.01	Quality management plans	Data quality improvement plan	Internal
APO14.05 Establish data profiling methodologies, processes and tools.	APO14.04	Data quality strategy	Data profiling methodologies, processes, practices, tools and results templates	Internal
APO14.06 Ensure a data quality assessment approach.	APO11.01	Quality management plans	Data quality assessment results	Internal
	APO14.04	Data quality strategy		
APO14.07 Define the data cleansing approach.	APO14.04	Data quality strategy	Data quality requirements	APO09.03
APO14.08 Manage the life cycle of data assets.	APO01.07	Data security and control guidelines		
	DSS04.07	Backup data		
APO14.09 Support data archiving and retention.	DSS06.05	Retention requirements	Data archive	Internal
APO14.10 Manage data backup and restore arrangements.	APO01.07	Data security and control guidelines	Backup test plan	DSS04.07
	APO14.01	Data management strategy	Backup plan	DSS04.07
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**
Data analysis	Skills Framework for the Information Age V6, 2015	DTAN
Data management	Skills Framework for the Information Age V6, 2015	DATM
Information assurance	Skills Framework for the Information Age V6, 2015	INAS
Information management	Skills Framework for the Information Age V6, 2015	IRMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Data cleansing policy	Outlines management's commitment to data cleansing. Prescribes frequency, guidelines and accountability; documents available methods, solutions and tools.	CMMI Data Management Maturity Model, 2014	Data Cleansing
Data management policy	Describes the organization's commitment to manage data assets across the data life cycle, from creation through delivery, maintenance and archiving.		
Data quality assessment policy	Describes the organization's data quality assurance assessment philosophy for ensuring the integrity of the data being used to make decisions that impact the organization. Assigns the frequency, guidelines and accountability for data quality assessment. Outlines available methods, solutions and tools.	(1) CMMI Data Management Maturity Model, 2014; (2) National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	(1) Data Quality Assessment; (2) 3.20 System and information integrity (SI-1)
Privacy policy	Documents the collection, use, disclosure and management of personal data. Personal data can be any data that may be used to identify an individual, including, but not limited to, name, address, date of birth, marital status, contact information, ID issue and expiry date, financial records, credit information, medical history, travel destination, and intent to acquire goods or services. The privacy policy defines how an enterprise collects, stores and releases personal information; how and when the client is informed of specific information that is collected and whether it is kept confidential, shared with partners, or sold to other firms or enterprises. The policy mandates compliance with relevant legislation related to data protection.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture of shared responsibility for the organization's data assets; acknowledge the potential value of data assets and ensure that roles and responsibilities are clear for governance and management of data assets.	CMMI Data Management Maturity Model, 2014	Data Governance
Create awareness around data integrity, accuracy, completeness and protection to establish a culture of data quality. Relate data quality to the enterprise's core values. Continuously communicate the impact and risk of data loss. Ensure that employees understand the true cost of failing to implement a data quality culture.	CMMI Data Management Maturity Model, 2014	Data Quality

G. Component: Services, Infrastructure and Applications
• Data modeling tools • Data repositories

4.3 Build, Acquire and Implement (BAI)

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI01 — Managed Programs	Focus Area: COBIT Core Model

Description

Manage all programs from the investment portfolio in alignment with enterprise strategy and in a coordinated way, based on a standard program management approach. Initiate, plan, control, and execute programs, and monitor expected value from the program.

Purpose

Realize desired business value and reduce the risk of unexpected delays, costs and value erosion. To do so, improve communications to and involvement of business and end users, ensure the value and quality of program deliverables and follow up of projects within the programs, and maximize program contribution to the 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 • 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	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
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
BAI01.01 Maintain a standard approach for program management. Maintain a standard approach for program 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 programs based on the defined standard approach b. Percent of stakeholders satisfied with program management

Activities	Capability Level
1. Maintain and enforce a standard approach to program 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. Put in place a program office or project management office (PMO) that maintains the standard approach for program and project management across the organization. The PMO supports all programs and projects by creating and maintaining required project documentation templates, providing training and best practices for program/project managers, tracking metrics on the use of best practices for project management, etc. In some cases the PMO may also report on program/project progress to senior management and/or stakeholders, help prioritize projects, and ensure all projects support the overall business objectives of the enterprise.	3
3. Evaluate lessons learned based on the use of the program management approach and update the approach accordingly.	4

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI01.02 Initiate a program. Initiate a program to confirm expected benefits and obtain authorization to proceed. This includes agreeing on program sponsorship, confirming the program mandate through approval of the conceptual business case, appointing program board or committee members, producing the program brief, reviewing and updating the business case, developing a benefits realization plan, and obtaining approval from sponsors to proceed.	a. Percent of I&T initiatives/projects championed by business owners b. Percent of strategic initiatives with assigned accountability c. Percent of programs undertaken without approved business cases d. Percent of stakeholders approving enterprise need, scope, planned outcome and level of program risk

Activities	Capability Level
1. Agree on program sponsorship. Appoint a program board/committee with members who have strategic interest in the program, responsibility for investment decision making, will be significantly impacted by the program and will be required to enable delivery of the change.	2
2. Appoint a dedicated manager for the program, with the commensurate competencies and skills to manage the program effectively and efficiently.	
3. Confirm the program mandate with sponsors and stakeholders. Articulate the strategic objectives for the program, potential strategies for delivery, improvement and benefits that are expected, and how the program fits with other initiatives.	3
4. Develop a detailed business case for a program. Involve all key stakeholders to develop and document a complete understanding of the expected enterprise outcomes, how they will be measured, the full scope of initiatives required, the risk involved and the impact on all aspects of the enterprise. Identify and assess alternative courses of action to achieve the desired enterprise outcomes.	
5. Develop a benefits realization plan that will be managed throughout the program to ensure that planned benefits always have owners and are achieved, sustained and optimized.	
6. Prepare the initial (conceptual) program business case, providing essential decision-making information regarding purpose, contribution to business objectives, expected value created, time frames, etc. Submit it for approval.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI01.03 Manage stakeholder engagement. Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information for 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 projects.	3
2. Identify, engage and manage stakeholders by establishing and maintaining appropriate levels of coordination, communication and liaison to ensure that they are involved in the program.	
3. Analyze stakeholder interests and requirements.	
4. Follow a defined process for collaborative agreements with respect to shared data and data usage within business processes.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 10. Project communications management
Management Practice	**Example Metrics**
BAI01.04 Develop and maintain the program plan. Formulate a program to lay the initial groundwork. Position it for successful execution by formalizing the scope of the work and identifying deliverables that will satisfy goals and deliver value. Maintain and update the program plan and business case throughout the full economic life cycle of the program, ensuring alignment with strategic objectives and reflecting the current status and insights gained to date.	a. Frequency of program status reviews that do not meet value criteria b. Percent of active programs undertaken without valid and updated program value maps

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Specify funding, cost, schedule and interdependencies of multiple projects.	2
2. Define and document the program plan covering all projects. Include what is needed to bring about changes to the enterprise; its purpose, mission, vision, values, culture, products and services; business processes; people skills and numbers; relationships with stakeholders, customers, suppliers and others; technology needs; and organizational restructuring required to achieve the program's expected enterprise outcomes.	3
3. Ensure that there is effective communication of program plans and progress reports among all projects and with the overall program. Ensure that any changes made to individual plans are reflected in the other enterprise program plans.	
4. Maintain the program plan to ensure that it is up to date and reflects alignment with current strategic objectives, actual progress and material changes to outcomes, benefits, costs and risk. Have the business drive the objectives and prioritize the work throughout to ensure that the program, as designed, will meet enterprise requirements. Review progress of individual projects and adjust the projects as necessary to meet scheduled milestones and releases.	
5. Throughout the program's economic life, update and maintain the business case and a benefits register to identify and define key benefits arising from undertaking the program.	
6. Prepare a program budget that reflects the full economic life cycle costs and the associated financial and nonfinancial benefits.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI01.05 Launch and execute the program. Launch and execute the program to acquire and direct the resources needed to accomplish the goals and benefits of the program as defined in the program plan. In accordance with stage-gate or release review criteria, prepare for stage-gate, iteration or release reviews to report progress and make the case for funding up to the following stage-gate or release review.	a. Percent of stakeholder sign-offs for stage-gate reviews of active programs b. Number of root cause analysis for deviations from the plan and necessary remedial actions addressed
Activities	**Capability Level**
1. Plan, resource and commission the necessary projects required to achieve the program results, based on funding review and approvals at each stage-gate review.	3
2. Manage each program or project to ensure that decision making and delivery activities are focused on value by achieving benefits for the business and goals in a consistent manner, addressing risk, and achieving stakeholder requirements.	
3. Establish agreed stages of the development process (development checkpoints). At the end of each stage, facilitate formal discussions of approved criteria with the stakeholders. After successful completion of functionality, performance and quality reviews, and before finalizing stage activities, obtain formal approval and sign-off from all stakeholders and the sponsor/ business process owner.	
4. Undertake a benefits realization process throughout the program to ensure that planned benefits always have owners and are likely to be achieved, sustained and optimized. Monitor benefits delivery and report against performance targets at the stage-gate or iteration and release reviews. Perform root cause analysis for deviations from the plan and identify and address any necessary remedial actions.	4
5. Plan audits, quality reviews, phase/stage-gate reviews and reviews of realized benefits.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI01.06 Monitor, control and report on the program outcomes. Monitor and control performance against plan throughout the full economic life cycle of the investment, covering solution delivery at the program level and value/outcome at the enterprise level. Report performance to the program steering committee and the sponsors.	a. Percent of expected program benefits achieved b. Percent of programs for which performance was monitored and timely remedial action taken when required

Activities	Capability Level
1. Update operational I&T portfolios to reflect changes that result from the program in the relevant I&T service, asset or resource portfolios.	3
2. Monitor and control the performance of the overall program and the projects within the program, including contributions of the business and IT to the projects. Report in a timely, complete and accurate fashion. Reporting may include schedule, funding, functionality, user satisfaction, internal controls and acceptance of accountabilities.	4
3. Monitor and control performance against enterprise and I&T strategies and goals. Report to management on enterprise changes implemented, benefits realized against the benefits realization plan and the adequacy of the benefits realization process.	
4. Monitor and control IT services, assets and resources created or changed as a result of the program. Note implementation and in-service dates. Report to management on performance levels, sustained service delivery and contribution to value.	
5. Manage program performance against key criteria (e.g., scope, schedule, quality, benefits realization, costs, risk, velocity), identify deviations from the plan and take timely remedial action when required.	
6. Monitor individual project performance related to delivery of the expected capabilities, schedule, benefits realization, costs, risk or other metric. Identify potential impacts on program performance and take timely remedial action when required.	
7. In accordance with stage-gate, release or iteration review criteria, undertake reviews to report on the progress of the program so that management can make go/no-go or adjustment decisions and approve further funding up to the following stage-gate, release or iteration.	

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

Management Practice	Example Metrics
BAI01.07 Manage program quality. Prepare and execute a quality management plan, processes and practices that align with quality management standards (QMS). Describe the approach to program quality and implementation. The plan should be formally reviewed and agreed on by all parties concerned and incorporated into the integrated program plan.	a. Percent of build-to-packages without errors b. Percent of program deliverables approved at each gate review

Activities	Capability Level
1. Identify assurance tasks and practices required to support the accreditation of new or modified systems during program planning, and include them in the integrated plans. Ensure that the tasks provide assurance that internal controls and security/privacy solutions meet the defined requirements.	3
2. To provide quality assurance for the program deliverables, identify ownership and responsibilities, quality review processes, success criteria and performance metrics.	
3. Define any requirements for independent validation and verification of the quality of deliverables in the plan.	4
4. Perform quality assurance and control activities in accordance with the quality management plan and QMS.	

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

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI01.08 Manage program risk. Eliminate or minimize specific risk associated with programs through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with the potential to cause unwanted change. Define and record any risk faced by program management.	a. Number of programs without a proper risk assessment b. Percent of programs aligned with the enterprise risk management framework
Activities	**Capability Level**
1. Establish a formal risk management approach aligned with the enterprise risk management (ERM) framework. Ensure that the approach includes identifying, analyzing, responding to, mitigating, monitoring and controlling risk.	3
2. Assign to appropriately skilled personnel the responsibility for executing the enterprise's risk management process within a program and ensuring 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 program is considered critical.	
3. Perform the risk assessment of identifying and quantifying risk continuously throughout the program. Manage and communicate risk appropriately within the program governance structure.	
4. Identify owners for actions to avoid, accept or mitigate risk.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI01.09 Close a program. Remove the program from the active investment portfolio when there is agreement that the desired value has been achieved or when it is clear it will not be achieved within the value criteria set for the program.	a. Percent of successfully closed programs that achieved desired value b. Time between program launch and detection of achievability of value
Activities	**Capability Level**
1. Bring the program to an orderly closure, including formal approval, disbanding of the program organization and supporting function, validation of deliverables, and communication of retirement.	3
2. Review and document lessons learned. Once the program is retired, remove it from the active investment portfolio. Move any resulting capabilities to an operational asset portfolio to ensure that value continues to be created and sustained.	4
3. Put accountability and processes in place to ensure that the enterprise continues to optimize value from the service, asset or resources. Additional investments may be required at some future time to ensure that this occurs.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	RS.IM Improvements

B. Component: Organizational Structures

Key Management Practice	Chief Executive Officer	Chief Risk Officer	Chief Information Officer	I&T Governance Board	Business Process Owners	Steering (Programs/Projects) Committee	Program Manager	Project Management Office	Head Architect	Head Development	Head IT Operations
BAI01.01 Maintain a standard approach for program management.	A		R	R			R				
BAI01.02 Initiate a program.		R			R	A	R	R			
BAI01.03 Manage stakeholder engagement.					R	A	R	R			
BAI01.04 Develop and maintain the program plan.						A	R	R			
BAI01.05 Launch and execute the program.			R		R	A	R	R			
BAI01.06 Monitor, control and report on the program outcomes.			R			A	R	R	R	R	R
BAI01.07 Manage program quality.					R	A	R	R			
BAI01.08 Manage program risk.		R			R	A	R	R		R	
BAI01.09 Close a program.			R		R	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
BAI01.01 Maintain a standard approach for program management.	APO03.04	• Implementation phase descriptions • Architecture governance requirements	Updated program management approaches	Internal
	APO05.04	Updated portfolios of programs, services and assets		
	APO10.04	Identified vendor delivery risk		
	EDM02.03	Requirements for stagegate reviews		
	EDM02.04	Actions to improve value delivery		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI01.02 Initiate a program.	**From**	**Description**	**Description**	**To**
	APO03.04	• Resource requirements • Implementation phase descriptions	Program mandate and brief	APO05.02
	APO05.02	Program business case	Program concept business case	APO05.02
	APO07.03	Skills and competencies matrix	Program benefit realization plan	APO05.02; APO06.05
	BAI05.02	Common vision and goals		
BAI01.03 Manage stakeholder engagement.			Results of stakeholder engagement effectiveness assessments	Internal
			Stakeholder engagement plan	Internal
BAI01.04 Develop and maintain the program plan.	APO05.02	Selected programs with ROI milestones	Program budget and benefits register	APO05.05; APO06.05
	APO07.03	Skills and competencies matrix	Resource requirements and roles	APO07.05; APO07.06
	APO07.05	Inventory of business and IT human resources	Program plan	Internal
	BAI05.02	Implementation team and roles		
	BAI05.03	Vision communication plan		
	BAI05.04	Identified quick wins		
	BAI07.03	Approved acceptance test plan		
	BAI07.05	Approved acceptance and release for production		
BAI01.05 Launch and execute the program.	BAI05.03	Vision communications	Results of program goal achievement monitoring	APO02.04
			Results of benefit realization monitoring	APO05.05; APO06.05
			Program audit plans	MEA04.02

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI01.06 Monitor, control and report on the program outcomes.	**From**	**Description**	**Description**	**To**
	APO05.01	Investment return expectations	Stage-gate review results	APO02.04; APO05.03; EDM02.02
	APO05.02	Business case assessments	Results of program performance reviews	MEA01.03
	APO05.03	Investment portfolio performance reports		
	APO05.05	• Benefit results and related communications • Corrective actions to improve benefit realization		
	APO07.05	• Resourcing shortfall analyses • Resource utilization records		
	BAI05.04	Communication of benefits		
	BAI06.03	Change request status reports		
	BAI07.05	Evaluation of acceptance results		
	EDM02.04	Feedback on portfolio and program performance		
BAI01.07 Manage program quality.	APO11.01	Quality management plans	Quality management plan	BAI02.04; BAI03.06; BAI07.01
	APO11.02	Customer requirements for quality management	Requirements for independent verification of deliverables	BAI07.03
BAI01.08 Manage program risk.	APO12.02	Risk analysis results	Program risk register	Internal
	BAI02.03	• Requirements risk register • Risk mitigation actions	Program risk assessment results	Internal
	Outside COBIT	Enterprise risk management (ERM) framework	Program risk management plan	Internal
BAI01.09 Close a program.	BAI07.08	• Post-implementation review report • Remedial action plan	Communication of program retirement and ongoing accountabilities	APO05.04; APO07.06
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 and 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**
Benefits management	Skills Framework for the Information Age V6, 2015	BENM
Business plan development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.3. Business Plan Development
Program management	Skills Framework for the Information Age V6, 2015	PGMG
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

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**
Ensure the organization understands and supports the value of enterprisewide program management. Establish an enterprisewide culture that supports consistent implementation of program management, taking into account organizational structure and business environment. Ensure the program office has a central view of all programs in the enterprise portfolio.		

G. Component: Services, Infrastructure and Applications
Program management tool

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI02 — Managed Requirements Definition	Focus Area: COBIT Core Model

Description

Identify solutions and analyze requirements before acquisition or creation to ensure that they align with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Coordinate the review of feasible options with affected stakeholders, including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.

Purpose

Create optimal solutions that meet enterprise needs while minimizing risk.

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	• AG05 Delivery of I&T services in line with business requirements • 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	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	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**
BAI02.01 Define and maintain business functional and technical requirements. Based on the business case, identify, prioritize, specify and agree on business information, functional, technical and control requirements covering the scope/understanding of all initiatives required to achieve the expected outcomes of the proposed I&T-enabled business solution.	a. Percent of requirements reworked due to misalignment with enterprise needs and expectations b. Percent of requirements validated through approaches such as peer review, model validation or operational prototyping

Activities	Capability Level
1. Ensure that all stakeholder requirements, including relevant acceptance criteria, are considered, captured, prioritized and recorded in a way that is understandable to all stakeholders, recognizing that the requirements may change and will become more detailed as they are implemented.	2
2. Express business requirements in terms of how the gap between current and desired business capabilities need to be addressed and how the user (employee, client, etc.) will interact with and use the solution.	
3. Specify and prioritize information, functional and technical requirements, based on the user experience design and confirmed stakeholder requirements.	
4. Ensure requirements meet enterprise policies and standards, enterprise architecture, strategic and tactical I&T plans, in-house and outsourced business and IT processes, security requirements, regulatory requirements, people competencies, organizational structure, business case, and enabling technology.	3
5. Include information control requirements in the business processes, automated processes and I&T environments to address information risk and to comply with laws, regulations and commercial contracts.	
6. Confirm acceptance of key aspects of the requirements, including enterprise rules, user experience, information controls, business continuity, legal and regulatory compliance, auditability, ergonomics, operability and usability, safety, confidentiality, and supporting documentation.	
7. Track and control scope, requirements and changes through the life cycle of the solution as understanding of the solution evolves.	
8. Define and implement a requirements definition and maintenance procedure and a requirements repository that are appropriate for the size, complexity, objectives and risk of the initiative that the enterprise is considering undertaking.	
9. Validate all requirements through approaches such as peer review, model validation or operational prototyping.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SD2.1 Specifications of Requirements
ISO/IEC 27002:2013/Cor.2:2015(E)	14.1 Security requirements of information systems
ITIL V3, 2011	Service Design, 5.1 Requirements engineering
PMBOK Guide Sixth Edition, 2017	Part 1: 5. Project scope management

Management Practice	Example Metrics
BAI02.02 Perform a feasibility study and formulate alternative solutions. Perform a feasibility study of potential alternative solutions, assess their viability and select the preferred option. If appropriate, implement the selected option as a pilot to determine possible improvements.	a. Percent of business case objectives met by proposed solution b. Percent of requirements satisfied by proposed solution

Activities	Capability Level
1. Identify required actions for solution acquisition or development based on the enterprise architecture. Take into account scope and/or time and/or budget limitations.	2
2. Review the alternative solutions with all stakeholders. Select the most appropriate one based on feasibility criteria, including risk and cost.	
3. Translate the preferred course of action into a high-level acquisition/development plan that identifies resources to be used and stages requiring a go/no-go decision.	3
4. Define and execute a feasibility study, pilot or basic working solution that clearly and concisely describes the alternative solutions and measures how these would satisfy the business and functional requirements. Include an evaluation of their technological and economic feasibility.	4

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

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI02.03 Manage requirements risk. Identify, document, prioritize and mitigate functional, technical and information processing-related risk associated with the enterprise requirements, assumptions and proposed solution.	a. Percent of requirements risk not covered by an appropriate risk response b. Level of detail of documented requirements risk c. Completeness of estimated probability and impact of listed requirements risk and risk responses

Activities	Capability Level
1. Identify quality, functional and technical requirements risk (due to, for example, lack of user involvement, unrealistic expectations, developers adding unnecessary functionality, unrealistic assumptions, etc.).	3
2. Determine appropriate risk response to requirements risk.	
3. Analyze the identified risk by estimating probability and impact on budget and schedule. Evaluate budgetary impact of appropriate risk response actions.	4

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

Management Practice	Example Metrics
BAI02.04 Obtain approval of requirements and solutions. Coordinate feedback from affected stakeholders. At predetermined key stages, obtain approval and sign-off from the business sponsor or product owner regarding functional and technical requirements, feasibility studies, risk analyses and recommended solutions.	a. Level of stakeholder satisfaction with requirements b. Number of solution exceptions to design noted during stage reviews c. Percent of stakeholders not approving solution in relation to business case

Activities	Capability Level
1. Ensure that the business sponsor or product owner makes the final choice of solution, acquisition approach and high-level design, according to the business case. Obtain necessary approvals from affected stakeholders (e.g., business process owner, enterprise architect, operations manager, security, privacy officer).	3
2. Obtain quality reviews throughout, and at the end of, each key project stage, iteration or release. Assess the results against the original acceptance criteria. Have business sponsors and other stakeholders sign off on each successful quality review.	4

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

B. Component: Organizational Structures														
Key Management Practice	**Chief Risk Officer**	**Chief Information Officer**	**Business Process Owners**	**Steering (Programs/Projects) Committee**	**Program Manager**	**Project Manager**	**Project Management Office**	**Relationship Manager**	**Head Architect**	**Head Development**	**Head IT Operations**	**Information Security Manager**	**Privacy Officer**
BAI02.01 Define and maintain business functional and technical requirements.			R	A	R	R	R	R	R	R		R	R
BAI02.02 Perform a feasibility study and formulate alternative solutions.			R	A	R	R	R			R			
BAI02.03 Manage requirements risk.	R	R	R	A	R	R	R			R	R	R	R
BAI02.04 Obtain approval of requirements and solutions.			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**
BAI02.01 Define and maintain business functional and technical requirements.	APO01.07	• Data classification guidelines • Data security and control guidelines • Data integrity procedures	Requirements definition repository	BAI03.01; BAI03.02; BAI03.12; BAI04.01; BAI05.01
	APO03.01	Architecture principles	Confirmed acceptance criteria from stakeholders	BAI03.01; BAI03.02; BAI03.12; BAI04.03; BAI05.01; BAI05.02
	APO03.02	• Baseline domain descriptions and architecture definition • Information architecture model	Record of requirement change requests	BAI03.09
	APO03.05	Solution development guidance		
	APO10.02	Vendor requests for information (RFIs) and requests for proposals (RFPs)		
	APO11.02	Acceptance criteria		
	APO14.02	Business glossary		
BAI02.02 Perform a feasibility study and formulate alternative solutions.	APO03.05	Solution development guidance	High-level acquisition/ development plan	APO10.02; BAI03.01
	APO10.01	Vendor catalog	Feasibility study report	BAI03.02; BAI03.03; BAI03.12
	APO10.02	• Vendor requests for information (RFIs) and requests for proposals (RFPs) • RFI and RFP evaluations • Decision results of vendor evaluations		
	APO11.02	Acceptance criteria		
BAI02.03 Manage requirements risk.			Requirements risk register	BAI01.08; BAI03.02; BAI04.01; BAI05.01; BAI11.06
			Risk mitigation actions	BAI01.08; BAI03.02; BAI05.01
BAI02.04 Obtain approval of requirements and solutions.	BAI01.07	Quality management plan	Approved quality reviews	APO11.03
	BAI11.05	Project quality management plan	Sponsor approvals of requirements and proposed solutions	BAI03.02; BAI03.03; BAI03.04

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 5. Project management scope: Inputs and Outputs

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Application design	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.6. Application Design
Business analysis	Skills Framework for the Information Age V6, 2015	BUAN
Business process improvement	Skills Framework for the Information Age V6, 2015	BPRE
Needs identification	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.11. Needs Identification
Requirements definition and management	Skills Framework for the Information Age V6, 2015	REQM
User experience analysis	Skills Framework for the Information Age V6, 2015	UNAN

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Software development policy	Standardizes software development across the organization by listing all protocols and standards to be followed.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture that ensures consistent and robust processes for defining requirements. Ensure that the processes clearly align development requirements with enterprise strategic requirements.		

G. Component: Services, Infrastructure and Applications
Requirements definition and documentation tools

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI03 — Managed Solutions Identification and Build	Focus Area: COBIT Core Model

Description

Establish and maintain identified products and services (technology, business processes and workflows) in line with enterprise requirements covering design, development, procurement/sourcing and partnering with vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.

Purpose

Ensure agile and scalable delivery of digital products and services. Establish timely and cost-effective solutions (technology, business processes and workflows) capable of supporting enterprise strategic and operational objectives.

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	• AG05 Delivery of I&T services in line with business requirements • 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	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	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
BAI03.01 Design high-level solutions. Develop and document high-level designs for the solution in terms of technology, business processes and workflows. Use agreed and appropriate phased or rapid Agile development techniques. Ensure alignment with the I&T strategy and enterprise architecture. Reassess and update the designs when significant issues occur during detailed design or building phases, or as the solution evolves. Apply a user-centric approach; ensure that stakeholders actively participate in the design and approve each version.	a. Number of design review deficiencies b. Percent of stakeholder participation in the design and approval signoff of each version

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Establish a high-level design specification that translates the proposed solution into a high-level design for business processes, supporting services, workflows, applications, infrastructure, and information repositories capable of meeting business and enterprise architecture requirements.	2
2. Involve appropriately qualified and experienced user experience designers and IT specialists in the design process to make sure that the design provides a solution that optimally uses the proposed I&T capabilities to enhance the business process.	
3. Create a design that complies with the organization's design standards. Ensure that it maintains a level of detail that is appropriate for the solution and development method and consistent with business, enterprise and I&T strategies, the enterprise architecture, security/privacy plan and applicable laws, regulations and contracts.	
4. After quality assurance approval, submit the final high-level design to the project stakeholders and the sponsor/business process owner for approval based on agreed criteria. This design will evolve throughout the project as understanding grows.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design
Management Practice	**Example Metrics**
BAI03.02 Design detailed solution components. Develop, document and elaborate detailed designs progressively. Use agreed and appropriate phased or rapid Agile development techniques, addressing all components (business processes and related automated and manual controls, supporting I&T applications, infrastructure services and technology products, and partners/suppliers). Ensure that the detailed design includes internal and external service level agreements (SLAs) and operational level agreements (OLAs).	a. Number of design review deficiencies b. Number of in-process design changes
Activities	**Capability Level**
1. Design progressively the business process activities and work flows that need to be performed in conjunction with the new application system to meet the enterprise objectives, including the design of the manual control activities.	2
2. Design the application processing steps. These steps include specification of transaction types and business processing rules, automated controls, data definitions/business objects, use cases, external interfaces, design constraints, and other requirements (e.g., licensing, legal, standards and internationalization/localization).	
3. Classify data inputs and outputs according to enterprise architecture standards. Specify the source data collection design. Document the data inputs (regardless of source) and validation for processing transactions as well as the methods for validation. Design the identified outputs, including data sources.	
4. Design the system/solution interface, including any automated data exchange.	
5. Design data storage, location, retrieval and recoverability.	
6. Design appropriate redundancy, recovery and backup.	
7. Design the interface between the user and the system application so that it is easy to use and self-documenting.	3
8. Consider the impact of the solution's need for infrastructure performance, being sensitive to the number of computing assets, bandwidth intensity and time sensitivity of the information.	
9. Proactively evaluate for design weaknesses (e.g., inconsistencies, lack of clarity, potential flaws) throughout the life cycle. Identify improvements when required.	
10. Provide an ability to audit transactions and identify root causes of processing errors.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI03.03 Develop solution components. Develop solution components progressively in a separate environment, in accordance with detailed designs following standards and requirements for development and documentation, quality assurance (QA), and approval. Ensure that all control requirements in the business processes, supporting I&T applications and infrastructure services, services and technology products, and partner/vendor services are addressed.	a. Number of solution exceptions to design noted during stage reviews b. Number of detailed designs for business processes, supporting services, applications and infrastructure, and information repositories

Activities	Capability Level
1. Within a separate environment, develop the proposed detailed design for business processes, supporting services, applications, infrastructure and information repositories.	2
2. When third-party providers are involved with the solution development, ensure that maintenance, support, development standards and licensing are addressed and adhered to in contractual obligations.	
3. Track change requests and design, performance and quality reviews. Ensure active participation of all impacted stakeholders.	
4. Document all solution components according to defined standards. Maintain version control over all developed components and associated documentation.	
5. Assess the impact of solution customization and configuration on the performance and efficiency of acquired solutions and on interoperability with existing applications, operating systems and other infrastructure. Adapt business processes as required to leverage the application capability.	3
6. Ensure that responsibilities for using high-security or restricted-access infrastructure components are clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SD1.2 System Development Environments
ISO/IEC 27002:2013/Cor.2:2015(E)	14.2 Security in development and support processes
ITIL V3, 2011	Service Strategy, 5.5 IT service strategy and application development
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-3)

Management Practice	Example Metrics
BAI03.04 Procure solution components. Procure solution components, based on the acquisition plan, in accordance with requirements and detailed designs, architecture principles and standards, and the enterprise's overall procurement and contract procedures, QA requirements, and approval standards. Ensure that all legal and contractual requirements are identified and addressed by the vendor.	a. Percent of suppliers certified b. Percent of suppliers engaged in collaborative design

Activities	Capability Level
1. Create and maintain a plan for the acquisition of solution components. Consider future flexibility for capacity additions, transition costs, risk and upgrades over the lifetime of the project.	3
2. Review and approve all acquisition plans. Consider risk, costs, benefits and technical conformance with enterprise architecture standards.	
3. Assess and document the degree to which acquired solutions require adaptation of business process to leverage the benefits of the acquired solution.	
4. Follow required approvals at key decision points during the procurement processes.	
5. Record receipt of all infrastructure and software acquisitions in an asset inventory.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SD2.3 Software Acquisition
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	3.4 Buying Decisions
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-4)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI03.05 Build solutions. Install and configure solutions and integrate with business process activities. During configuration and integration of hardware and infrastructure software, implement control, security, privacy and auditability measures to protect resources and ensure availability and data integrity. Update the product or services catalogue to reflect the new solutions.	a. Gap between estimated and final development effort b. Number of software problems reported c. Number of review errors

Activities	Capability Level
1. Integrate and configure business and IT solution components and information repositories in line with detailed specifications and quality requirements. Consider the role of users, business stakeholders and the process owner in the configuration of business processes.	2
2. Complete and update business process and operational manuals, where necessary, to account for any customization or special conditions unique to the implementation.	
3. Consider all relevant information control requirements in solution component integration and configuration. Include implementation of business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorized and auditable.	
4. Implement audit trails during configuration and integration of hardware and infrastructural software to protect resources and ensure availability and integrity.	3
5. Consider when the effect of cumulative customizations and configurations (including minor changes that were not subjected to formal design specifications) requires a high-level reassessment of the solution and associated functionality.	
6. Configure acquired application software to meet business processing requirements.	
7. Define product and service catalogues for relevant internal and external target groups, based on business requirements.	
8. Ensure the interoperability of solution components with supporting tests, preferably automated.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
HITRUST CSF version 9, September 2017	10.05 Security in Development & Support Processes
ISF, The Standard of Good Practice for Information Security 2016	SD2.4 System Build

Management Practice	Example Metrics
BAI03.06 Perform quality assurance (QA). Develop, resource and execute a QA plan aligned with the QMS to obtain the quality specified in the requirements definition and in the enterprise's quality policies and procedures.	a. Number of reworked solution designs due to misalignment with requirements b. Number and robustness of documented monitor activities performed

Activities	Capability Level
1. Define a QA plan and practices include, for example, specification of quality criteria, validation and verification processes, definition of how quality will be reviewed, necessary qualifications of quality reviewers, and roles and responsibilities for the achievement of quality.	3
2. Frequently monitor the solution quality based on project requirements, enterprise policies, adherence to development methodologies, quality management procedures and acceptance criteria.	4
3. Employ, as appropriate, code inspection, test-driven development practices, automated testing, continuous integration, walk-throughs and testing of applications. Report on outcomes of the monitoring process and testing to the application software development team and IT management.	
4. Monitor all quality exceptions and address all corrective actions. Maintain a record of all reviews, results, exceptions and corrections. Repeat quality reviews, where appropriate, based on the amount of rework and corrective action.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SD1.3 Quality Assurance

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI03.07 Prepare for solution testing. Establish a test plan and required environments to test the individual and integrated solution components. Include the business processes and supporting services, applications and infrastructure.	a. Number of business users involved in creating a test plan b. Number and robustness of use cases created for testing

Activities	Capability Level
1. Create an integrated test plan and practices commensurate with the enterprise environment and strategic technology plans. Ensure that the integrated test plan and practices will enable the creation of suitable testing and simulation environments to help verify that the solution will operate successfully in the live environment and deliver the intended results and that controls are adequate.	2
2. Create a test environment that supports the full scope of the solution. Ensure that the test environment reflects, as closely as possible, real-world conditions, including the business processes and procedures, range of users, transaction types, and deployment conditions.	
3. Create test procedures that align with the plan and practices and allow evaluation of the operation of the solution in real-world conditions. Ensure that the test procedures evaluate the adequacy of the controls, based on enterprisewide standards that define roles, responsibilities and testing criteria, and are approved by project stakeholders and the sponsor/business process owner.	3
4. Document and save the test procedures, cases, controls and parameters for future testing of the application.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	AD.DE Safeguard Development Environment
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
BAI03.08 Execute solution testing. During development, execute testing continually (including control testing), in accordance with the defined test plan and development practices in the appropriate environment. Engage business process owners and end users in the test team. Identify, log and prioritize errors and issues identified during testing.	a. Number of errors found during testing b. Time and effort to complete tests

Activities	Capability Level
1. Undertake testing of solutions and their components in accordance with the testing plan. Include testers independent from the solution team, with representative business process owners and end users. Ensure that testing is conducted only within the development and test environments.	2
2. Use clearly defined test instructions, as defined in the test plan. Consider the appropriate balance between automated scripted tests and interactive user testing.	
3. Undertake all tests in accordance with the test plan and practices. Include the integration of business processes and IT solution components and of nonfunctional requirements (e.g., security, privacy, interoperability, usability).	
4. Identify, log and classify (e.g., minor, significant and mission-critical) errors during testing. Repeat tests until all significant errors have been resolved. Ensure that an audit trail of test results is maintained.	
5. Record testing outcomes and communicate results of testing to stakeholders in accordance with the test plan.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	
CMMI Cybermaturity Platform, 2018	AD.ST Secure Development Testing
ISF, The Standard of Good Practice for Information Security 2016	SD2.5 System Testing; SD2.6 Security Testing
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-11)

A. Component: Process *(cont.)*		
Management Practice	**Example Metrics**	
BAI03.09 Manage changes to requirements. Track the status of individual requirements (including all rejected requirements) throughout the project life cycle. Manage the approval of changes to requirements.	a. Number of tracked, approved changes that generate new errors b. Percent of stakeholders satisfied with change management processes	
Activities		**Capability Level**
1. Assess the impact of all solution change requests on the solution development, the original business case and the budget. Categorize and prioritize them accordingly.		3
2. Track changes to requirements, enabling all stakeholders to monitor, review and approve the changes. Ensure that the outcomes of the change process are fully understood and agreed on by all the stakeholders and the sponsor/business process owner.		
3. Apply change requests, maintaining the integrity of integration and configuration of solution components. Assess the impact of any major solution upgrade and classify it according to agreed objective criteria (such as enterprise requirements), based on the outcome of analysis of the risk involved (such as impact on existing systems and processes or security/privacy), cost-benefit justification and other requirements.		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ISF, The Standard of Good Practice for Information Security 2016	SD2.9 Post-implementation Review	
Management Practice	**Example Metrics**	
BAI03.10 Maintain solutions. Develop and execute a plan for the maintenance of solution and infrastructure components. Include periodic reviews against business needs and operational requirements.	a. Number of demands for maintenance that are not satisfied b. Duration of demands for maintenance that are satisfied and that go unsatisfied	
Activities		**Capability Level**
1. Develop and execute a plan for the maintenance of solution components. Include periodic reviews against business needs and operational requirements such as patch management, upgrade strategies, risk, privacy, vulnerabilities assessment and security requirements.		2
2. Assess the significance of a proposed maintenance activity on current solution design, functionality and/or business processes. Consider risk, user impact and resource availability. Ensure that business process owners understand the effect of designating changes as maintenance.		3
3. In the event of major changes to existing solutions that result in significant change in current designs and/or functionality and/or business processes, follow the development process used for new systems. For maintenance updates, use the change management process.		
4. Ensure that the pattern and volume of maintenance activities are analyzed periodically for abnormal trends that indicate underlying quality or performance problems, cost/benefit of major upgrade, or replacement in lieu of maintenance.		4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ISO/IEC 27002:2013/Cor.2:2015(E)	14.3 Test data	
Management Practice	**Example Metrics**	
BAI03.11 Define IT products and services and maintain the service portfolio. Define and agree on new or changed IT products or services and service level options. Document new or changed product and service definitions and service level options to be updated in the products and services portfolio.	a. Percent of stakeholders signing off on new I&T services b. Percent of new or changed service definitions and service level options documented in the services portfolio. c. Percent of new or changed service definitions and service level options updated in the services portfolio	

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Propose definitions of the new or changed IT products and services to ensure that they are fit for purpose. Document the proposed definitions in the portfolio list of products and services to be developed.	3
2. Propose new or changed service level options (service times, user satisfaction, availability, performance, capacity, security, privacy, continuity, compliance and usability) to ensure that the IT products and services are fit for use. Document the proposed service options in the portfolio.	
3. Interface with business relationship management and portfolio management to agree on the proposed product and service definitions and service level options.	
4. If product or service change falls within agreed approval authority, build the new or changed IT products and services or service level options. Otherwise, pass the change to portfolio management for investment review.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI03.12 Design solutions based on the defined development methodology. Design, develop and implement solutions with the appropriate development methodology (i.e., waterfall, Agile or bimodal I&T), in accordance with the overall strategy and requirements.	a. Percent of solution development projects that apply selected development methodologies b. Percent of processes adapted to the chosen strategy
Activities	**Capability Level**
1. Analyze and assess the impact of choosing a development methodology (i.e., waterfall, Agile, bimodal) on the available resources, architecture requirements, configuration settings and system rigidity.	3
2. Establish the appropriate development methodology and organizational approach that delivers the proposed solution efficiently and effectively and that is capable of meeting business, architecture and system requirements. Adapt processes as required to the chosen strategy.	
3. Establish the needed project teams as defined by the chosen development methodology. Provide sufficient training.	
4. Consider applying a dual system, if required, in which cross-functional groups (digital factories) focus on developing one product or process using a different technology, operational, or managerial methodology from the rest of the company. Embedding these groups in business units has the advantage of spreading the new culture of agile development and making this digital factory approach the norm.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD1.1 System Development Methodology

B. Component: Organizational Structures																				
Key Management Practice	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	Business Process Owners	Portfolio Manager	Steering (Programs/Projects) Committee	Program Manager	Project Manager	Project Management Office	Relationship Manager	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI03.01 Design high-level solutions.		R		R		A	R	R	R	R		R				R		
BAI03.02 Design detailed solution components.		R		R		A	R	R	R			R						
BAI03.03 Develop solution components.		R		R		A	R	R	R			R						
BAI03.04 Procure solution components.		R		R		A						R	R	R				
BAI03.05 Build solutions.		R		R		A	R	R	R			R				R		
BAI03.06 Perform quality assurance (QA).		R		R		A	R	R	R			R						
BAI03.07 Prepare for solution testing.		R		R		A						R	R		R	R	R	R
BAI03.08 Execute solution testing.		R		R		A						R	R			R		R
BAI03.09 Manage changes to requirements.		R		R		A	R	R	R		R	R				R		R
BAI03.10 Maintain solutions.	A	R		R			R	R	R			R				R		R
BAI03.11 Define IT products and services and maintain the service portfolio.	A														R	R		R
BAI03.12 Design solutions based on the defined development methodology.	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**	
BAI03.01 Design high-level solutions.	**From**	**Description**	**Description**	**To**
	APO03.01	Architecture principles	Approved high-level design specification	BAI04.03; BAI05.01
	APO03.02	Baseline domain descriptions and architecture definition		
	APO04.03	Research analyses of innovation possibilities		
	APO04.04	Evaluations of innovation ideas		
	BAI02.01	• Requirements definition repository • Confirmed acceptance criteria from stakeholders		
	BAI02.02	High-level acquisition/ development plan		
BAI03.02 Design detailed solution components.	APO03.01	Architecture principles	Internal and external SLAs	BAI04.02
	APO03.02	• Baseline domain descriptions and architecture definition • Information architecture model	Approved detailed design specification	BAI04.03; BAI05.01
	APO03.05	Solution development guidance		
	APO04.06	Assessments of innovative approaches		
	BAI02.01	• Requirements definition repository • Confirmed acceptance criteria from stakeholders		
	BAI02.02	Feasibility study report		
	BAI02.03	• Requirements risk register • Risk mitigation actions		
	BAI02.04	Approvals of requirements and proposed solutions by sponsor		
BAI03.03 Develop solution components.	BAI02.02	Feasibility study report	Documented solution components	BAI04.03; BAI05.05; BAI08.02; BAI08.03
	BAI02.04	Approvals of requirements and proposed solutions by sponsor		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI03.04 Procure solution components.	**From**	**Description**	**Description**	**To**
	BAI02.04	Approvals of requirements and proposed solutions by sponsor	Approved acquisition plan	APO10.03
			Updates to asset inventory	BAI09.01
BAI03.05 Build solutions.			Integrated and configured solution components	BAI06.01
BAI03.06 Perform quality assurance (QA).	APO11.01	Results of QMS effectiveness reviews	Quality review results, exceptions and corrections	APO11.04
	BAI01.07	Quality management plan	Quality assurance plan	APO11.04
	BAI11.05	Project quality management plan		
BAI03.07 Prepare for solution testing.			Test procedures	BAI07.03
			Test plan	BAI07.03
BAI03.08 Execute solution testing.	APO04.05	Analysis of rejected initiatives	Test result communications	BAI07.03
			Test result logs and audit trails	BAI07.03
BAI03.09 Manage changes to requirements.	APO04.05	Results and recommendations from proof-of-concept initiatives	Record of all approved and applied change requests	BAI06.03
	BAI02.01	Record of requirement change requests		
BAI03.10 Maintain solutions.			Maintenance plan	APO08.05
			Updated solution components and related documentation	BAI05.05
BAI03.11 Define IT products and services and maintain the service portfolio.	APO02.04	• Gaps and changes required to realize target capability • Value benefit statement for target environment	Updated service portfolio	APO05.04
	APO06.02	Budget allocations	Service definitions	EDM02.01; DSS01.03
	APO06.03	• I&T budget • Budget communications		
	APO08.05	Definition of potential improvement projects		
	BAI10.02	Configuration baseline		
	BAI10.03	Approved changes to baseline		
	BAI10.04	Configuration status reports		
	EDM04.01	Guiding principles for allocating resources and capabilities		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI03.12 Design solutions based on the defined development methodology.	**From**	**Description**	**Description**	**To**
	APO03.02	Baseline domain descriptions and architecture definition		
	APO03.05	Solution development guidance		
	APO07.03	Skills and competencies matrix		
	BAI02.01	• Confirmed acceptance criteria from stakeholders • Requirements definition repository		
	BAI02.02	Feasibility study report		
	BAI10.02	Configuration baseline		
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 development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.1. Application Development
Business process testing	Skills Framework for the Information Age V6, 2015	BPTS
Component integration	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.2. Component Integration
Database design	Skills Framework for the Information Age V6, 2015	DBDS
Documentation production	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.5. Documentation Production
Hardware design	Skills Framework for the Information Age V6, 2015	HWDE
Porting/software configuration	Skills Framework for the Information Age V6, 2015	PORT
Programming/software development	Skills Framework for the Information Age V6, 2015	PROG
Release and deployment	Skills Framework for the Information Age V6, 2015	RELM
Solution architecture	Skills Framework for the Information Age V6, 2015	ARCH
Solution deployment	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.4. Solution Deployment
Systems design	Skills Framework for the Information Age V6, 2015	DESN
Systems development management	Skills Framework for the Information Age V6, 2015	DLMG
Systems engineering	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.6. Systems Engineering

D. Component: People, Skills and Competencies *(cont.)*		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Systems installation/ decommissioning	Skills Framework for the Information Age V6, 2015	HSIN
Systems integration	Skills Framework for the Information Age V6, 2015	SINT
Testing	Skills Framework for the Information Age V6, 2015	TEST
Testing	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.3. Testing
User experience design	Skills Framework for the Information Age V6, 2015	HCEV

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Maintenance policy	Defines proper support of software and hardware components to ensure longer asset life, increase employee productivity and maintain an acceptable user experience.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.10 Maintenance (MA-1)
Software development policy	Standardizes software development across the organization by listing all protocols and standards to be followed.		
System and service acquisition policy	Provides procedures to assess, review and validate requirements for acquisition of system and services.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-1)

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Ensure agile and scalable delivery of digital services; engage an ecosystem of partners with whom the organization can work or set up a bimodal IT structure with digital factories, agile leaders and teams, continuous flow, and a mindset toward improvement.		
Establish an open, unbiased culture that fairly and objectively evaluates alternatives when investigating potential new solutions (including whether to build or buy).		

G. Component: Services, Infrastructure and Applications
• Digital factory services, separating “fast IT” (the digital factory responsible for developing digital applications) from legacy core IT • Solution evaluation and selection services • Testing tools and services

Domain: Build, Acquire and Implement Management Objective: BAI04 — Managed Availability and Capacity	Focus Area: COBIT Core Model

Description

Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.

Purpose

Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.

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
BAI04.01 Assess current availability, performance and capacity and create a baseline. Assess availability, performance and capacity of services and resources to ensure that cost-justifiable capacity and performance are available to support business needs and deliver against service level agreements (SLAs). Create availability, performance and capacity baselines for future comparison.	a. Percent of actual capacity usage b. Percent of actual availability c. Percent of actual performance

Activities	Capability Level
1. Consider the following (current and forecasted) in the assessment of availability, performance and capacity of services and resources: customer requirements, business priorities, business objectives, budget impact, resource utilization, IT capabilities and industry trends.	2
2. Identify and follow up on all incidents caused by inadequate performance or capacity.	3
3. Monitor actual performance and capacity usage against defined thresholds, supported, where necessary, with automated software.	4
4. Regularly evaluate the current levels of performance for all processing levels (business demand, service capacity and resource capacity) by comparing them against trends and SLAs. Take into account changes in the environment.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	DP.CP Capacity Planning
ISF, The Standard of Good Practice for Information Security 2016	SY2.2 Performance and Capacity Management
ISO/IEC 20000-1:2011(E)	6.5 Capacity management
ITIL V3, 2011	Service Design, 4.4 Availability Management; 4.5 Capacity Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-10, PL-11)

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI04.02 Assess business impact. Identify important services to the enterprise. Map services and resources to business processes and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. For vital business functions, ensure that availability requirements can be satisfied per service level agreement (SLA).	a. Number of scenarios created to assess future availability situations b. Percent of business process owners signing off on analysis results

Activities	Capability Level
1. Identify only those solutions or services that are critical in the availability and capacity management process.	2
2. Map the selected solutions or services to the application(s) and infrastructure (IT and facility) on which they depend to enable a focus on critical resources for availability planning.	3
3. Collect data on availability patterns from logs of past failures and performance monitoring. Use modeling tools that help predict failures based on past usage trends and management expectations of new environment or user conditions.	4
4. Based on the collected data, create scenarios that describe future availability situations to illustrate a variety of potential capacity levels needed to achieve the availability performance objective.	
5. Based on the scenarios, determine the likelihood that the availability performance objective will not be achieved.	
6. Determine the impact of the scenarios on the business performance measures (e.g., revenue, profit, customer services). Engage the business-line, functional (especially finance) and regional leaders to understand their evaluation of impact.	
7. Ensure that business process owners fully understand and agree to the results of this analysis. From the business owners, obtain a list of unacceptable risk scenarios that require a response to reduce risk to acceptable levels.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	6.3 Service continuity and availability management

Management Practice	Example Metrics
BAI04.03 Plan for new or changed service requirements. Plan and prioritize availability, performance and capacity implications of changing business needs and service requirements.	a. Number of unplanned capacity, performance or availability upgrades b. Percent that management performs comparisons of actual demand on resources against forecasted supply and demand

Activities	Capability Level
1. Identify availability and capacity implications of changing business needs and improvement opportunities. Use modeling techniques to validate availability, performance and capacity plans.	3
2. Review availability and capacity implications of service trend analysis.	4
3. Ensure that management performs comparisons of actual demand on resources against forecasted supply and demand to evaluate current forecasting techniques and make improvements where possible.	
4. Prioritize needed improvements and create cost-justifiable availability and capacity plans.	5
5. Adjust the performance and capacity plans and SLAs based on realistic, new, proposed and/or projected business processes and supporting services, applications and infrastructure changes. Also include reviews of actual performance and capacity usage, including workload levels.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	5. Design and transition of new changed services

Management Practice	Example Metrics
BAI04.04 Monitor and review availability and capacity. Monitor, measure, analyze, report and review availability, performance and capacity. Identify deviations from established baselines. Review trend analysis reports identifying any significant issues and variances. Initiate actions where necessary and ensure that all outstanding issues are addressed.	a. Number of events exceeding planned limits for capacity b. Number of transaction peaks exceeding target performance

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Provide capacity reports to the budgeting processes.	2
2. Establish a process for gathering data to provide management with monitoring and reporting information for availability, performance and capacity workload of all I&T-related resources.	3
3. Provide regular reporting of the results in an appropriate form for review by IT and business management and communication to enterprise management.	4
4. Integrate monitoring and reporting activities in the iterative capacity management activities (monitoring, analysis, tuning and implementations).	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI04.05 Investigate and address availability, performance and capacity issues. Address deviations by investigating and resolving identified availability, performance and capacity issues.	a. Number and percentage of unresolved availability, performance and capacity issues b. Number of availability incidents
Activities	**Capability Level**
1. Obtain guidance from vendor product manuals to ensure an appropriate level of performance availability for peak processing and workloads.	3
2. Define an escalation procedure for swift resolution in case of emergency capacity and performance problems.	
3. Identify performance and capacity gaps based on monitoring current and forecasted performance. Use the known availability, continuity and recovery specifications to classify resources and allow prioritization.	4
4. Define corrective actions (e.g., shifting workload, prioritizing tasks or adding resources when performance and capacity issues are identified).	5
5. Integrate required corrective actions into the appropriate planning and change management processes.	
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 Information Officer**	**Chief Technology Officer**	**Business Process Owners**	**Head Architect**	**Head IT Operations**	**Service Manager**	**Business Continuity Manager**
BAI04.01 Assess current availability, performance and capacity and create a baseline.		R	A	R		R	R	
BAI04.02 Assess business impact.	A			R		R	R	
BAI04.03 Plan for new or changed service requirements.		R	A	R		R	R	
BAI04.04 Monitor and review availability and capacity.	A			R		R	R	
BAI04.05 Investigate and address availability, performance and capacity issues.		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**
BAI04.01 Assess current availability, performance and capacity and create a baseline.	BAI02.01	Requirements definition repository	Evaluations against SLAs	APO09.05
	BAI02.03	Requirements risk register	Availability, performance and capacity baselines	Internal
BAI04.02 Assess business impact.	BAI03.02	Internal and external service level agreements (SLAs)	Availability, performance and capacity business impact assessments	Internal
			Availability, performance and capacity scenarios	Internal
BAI04.03 Plan for new or changed service requirements.	BAI02.01	Confirmed acceptance criteria from stakeholders	Performance and capacity plans	APO02.02
	BAI03.01	Approved high-level design specification	Prioritized improvements	APO02.02
	BAI03.02	Approved detailed design specification		
	BAI03.03	Documented solution components		
BAI04.04 Monitor and review availability and capacity.			Availability, performance and capacity monitoring review reports	MEA01.03
BAI04.05 Investigate and address availability, performance and capacity issues.			Corrective actions	APO02.02
			Emergency escalation procedure	DSS02.02
			Performance and capacity gaps	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**
Availability management	Skills Framework for the Information Age V6, 2015	AVMT
Capacity management	Skills Framework for the Information Age V6, 2015	CPMG

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Availability management policy	Informs infrastructure planning in terms of availability, scalability, reliability and potentially resilience. Includes guidelines to identify bandwidth, capacity and availability of services (prior to design and provisioning), establish service level agreements (SLAs), and implement continuous monitoring of circuits, traffic and response times.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
For enterprises that depend on information, availability and capacity management are critical to successful operations. Establish a culture in which product and service availability and capacity are prioritized (in line with business requirements) and supported by processes and behaviors that not only identify required availability and capacity before design, but also consider them in provisioning. Consistently define smart SLAs; continuously monitor circuits, traffic and response times; perform regular testing for business continuity and disaster recovery of infrastructure.		

G. Component: Services, Infrastructure and Applications
• Capacity planning tools • Provisioning services and tools • Service level monitoring tools

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI05 — Managed Organizational Change	Focus Area: COBIT Core Model

Description

Maximize the likelihood of successfully implementing sustainable enterprisewide organizational change quickly and with reduced risk. Cover the complete life cycle of the change and all affected stakeholders in the business and IT.

Purpose

Prepare and commit stakeholders for business change and reduce the risk of failure.

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	• AG03 Realized benefits from I&T-enabled investments and services portfolio • AG08 Enabling and supporting business processes by integrating applications and technology • 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
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	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
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	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
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
BAI05.01 Establish the desire to change. Understand the scope and impact of the desired change. Assess stakeholder readiness and willingness to change. Identify actions that will motivate stakeholder acceptance and participation to make the change work successfully.	a. Level of senior management involvement b. Level of stakeholder desire for the change

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Assess the scope and impact of the envisioned change, the various stakeholders who are affected, the nature of the impact on and involvement required from each stakeholder group, and the current readiness and ability to adopt the change.	2
2. To establish the desire to change, identify, leverage and communicate current pain points, negative events, risk, customer dissatisfaction and business problems, as well as initial benefits, future opportunities and rewards, and competitive advantages.	
3. Issue key communications from the executive committee or CEO to demonstrate commitment to the change.	
4. Provide visible leadership from senior management to establish direction and to align, motivate and inspire stakeholders to desire the change.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Define your change management strategy
Management Practice	**Example Metrics**
BAI05.02 Form an effective implementation team. Establish an effective implementation team by assembling appropriate members, creating trust, and establishing common goals and effectiveness measures.	a. Number of identified skills or capacity issues in implementation team b. Stakeholder satisfaction ratings of implementation team
Activities	**Capability Level**
1. Identify and assemble an effective core implementation team that includes appropriate members from business and IT with the capacity to spend the required amount of time and contribute knowledge and expertise, experience, credibility, and authority. Consider including external parties such as consultants to provide an independent view or to address skill gaps. Identify potential change agents within different parts of the enterprise with whom the core team can work to support the vision and cascade changes.	3
2. Create trust within the core implementation team through carefully planned events with effective communication and joint activities.	
3. Develop a common vision and goals that support the enterprise objectives.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Prepare your change management team
Management Practice	**Example Metrics**
BAI05.03 Communicate desired vision. Communicate the desired vision for the change in the language of those affected by it. The communication should be made by senior management and include the rationale for, and benefits of, the change; the impacts of not making the change; and the vision, the road map and the involvement required of the various stakeholders.	a. Number of questions with regards to the change b. Stakeholder feedback on level of understanding of the change
Activities	**Capability Level**
1. Develop a vision communication plan to address the core audience groups, their behavioral profiles and information requirements, communication channels, and principles.	3
2. Deliver the communication at appropriate levels of the enterprise, in accordance with the plan.	
3. Reinforce the communication through multiple forums and repetition.	
4. Make all levels of leadership accountable for demonstrating the vision.	
5. Check understanding of the desired vision and respond to any issues highlighted by staff.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI05.04 Empower role players and identify short-term wins. Empower those with implementation roles by assigning accountability. Provide training and align organizational structures and HR processes. Identify and communicate short-term wins that are important from a change-enablement perspective.	a. Level of satisfaction of role players operating, using and maintaining the change b. Percent of role players trained c. Percent of role players with appropriate assigned authority d. Role player feedback on level of empowerment e. Role player self-assessment of relevant capabilities

Activities	Capability Level
1. Plan the training opportunities staff will need to develop the appropriate skills and attitudes to feel empowered.	2
2. Identify, prioritize and deliver opportunities for quick wins. These could be related to current known areas of difficulty or external factors that need to be addressed urgently.	
3. Leverage delivered quick wins by communicating the benefits to those impacted to show the vision is on track. Fine-tune the vision, keep leaders on board and build momentum.	
4. Identify organizational structures compatible with the vision; if required, make changes to ensure alignment.	3
5. Align HR processes and measurement systems (e.g., performance evaluation, compensation decisions, promotion decisions, recruiting and hiring) to support the vision.	
6. Identify and manage leaders who continue to resist needed change.	

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

Management Practice	Example Metrics
BAI05.05 Enable operation and use. Plan and implement all technical, operational and usage aspects so all those who are involved in the future state environment can exercise their responsibility.	a. Percent of users appropriately empowered for the change b. Percent of plans developed for operation and use of the change

Activities	Capability Level
1. Develop a plan for operation and use of the change. The plan should communicate and build on realized quick wins, address behavioral and cultural aspects of the broader transition, and increase buy-in and engagement. Ensure that the plan covers a holistic view of the change and provides documentation (e.g., procedures), mentoring, training, coaching, knowledge transfer, enhanced immediate post-go-live support and ongoing support.	3
2. Implement the operation and use plan. Define and track success measures, including hard business measures and perception measures that indicate how people feel about a change. Take remedial action as necessary.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PROSCI® 3-Phase Change Management Process	Phase 2. Managing change

Management Practice	Example Metrics
BAI05.06 Embed new approaches. Embed new approaches by tracking implemented changes, assessing the effectiveness of the operation and use plan, and sustaining ongoing awareness through regular communication. Take corrective measures as appropriate (which may include enforcing compliance).	a. Level of satisfaction of users with adoption of the change b. Percent of compliance audits which identified root causes for low adoption c. Number of compliance audits conducted to identify root causes for low adoption and recommended corrective action

Activities	Capability Level
1. Make process owners accountable for normal day-to-day operations.	2
2. Celebrate successes and implement reward and recognition programs to reinforce the change.	3
3. Provide ongoing awareness through regular communication of the change and its adoption.	
4. Use performance measurement systems to identify root causes for low adoption. Take corrective action.	4
5. Conduct compliance audits to identify root causes for low adoption. Recommend corrective action.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI05.07 Sustain changes. Sustain changes through effective training of new staff, ongoing communication campaigns, continued commitment of top management, monitoring of adoption and sharing of lessons learned across the enterprise.	a. Number of trainings and knowledge transfers performed b. Percent of top management engagement towards reinforcing the change

Activities	Capability Level
1. Sustain and reinforce the change through regular communication that demonstrates top management commitment.	2
2. Provide mentoring, training, coaching and knowledge transfer to new staff to sustain the change.	3
3. Perform periodic reviews of the operation and use of the change. Identify improvements.	4
4. Capture lessons learned relating to implementation of the change. Share knowledge across the enterprise.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change

B. Component: Organizational Structures																		
Key Management Practice	Executive Committee	Chief Executive Officer	Chief Operating Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Business Process Owners	Program Manager	Project Manager	Project Management Office	Head Human Resources	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager
BAI05.01 Establish the desire to change.	R	A		R	R	R	R	R	R	R		R					
BAI05.02 Form an effective implementation team.	A			R	R	R			R	R	R		R				
BAI05.03 Communicate desired vision.	A			R	R	R	R		R	R							
BAI05.04 Empower role players and identify short-term wins.	A			R	R	R			R	R		R					
BAI05.05 Enable operation and use.	A		R	R	R	R		R			R		R	R	R	R	R
BAI05.06 Embed new approaches.	A		R	R	R	R		R			R		R	R	R	R	R
BAI05.07 Sustain changes.	A		R	R	R	R		R	R	R	R		R	R	R	R	R
Related Guidance (Standards, Frameworks, Compliance Requirements)																	
No related guidance for this component																	

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
BAI05.01 Establish the desire to change.	**From**	**Description**	**Description**	**To**
	APO11.02	Results of quality of service, including customer feedback	Communications from executive management committing to change	Internal
	BAI02.01	• Requirements definition repository • Confirmed acceptance criteria from stakeholders	Communications of drivers for change	Internal
	BAI02.03	• Requirements risk register • Risk mitigation actions		
	BAI03.01	Approved high-level design specification		
	BAI03.02	Approved detailed design specification		
BAI05.02 Form an effective implementation team.	BAI02.01	Confirmed acceptance criteria from stakeholders	Common vision and goals	BAI01.02
			Implementation team and roles	BAI01.04
BAI05.03 Communicate desired vision.			Vision communication plan	BAI01.04
			Vision communications	BAI01.05
BAI05.04 Empower role players and identify short-term wins.	Outside COBIT	Enterprise organizational structure	Aligned HR performance objectives	APO07.04
			Identified quick wins	BAI01.04
			Communication of benefits	BAI01.06
BAI05.05 Enable operation and use.	BAI03.03	Documented solution components	Operation and use plan	APO08.04; BAI08.03; DSS01.01; DSS01.02; DSS06.02
	BAI03.10	Updated solution components and related documentation	Success measures and results	APO08.05; BAI07.07; BAI07.08; MEA01.03
BAI05.06 Embed new approaches.			HR performance review results	APO07.04
			Awareness communications	Internal
			Compliance audit results	MEA02.02; MEA03.03
BAI05.07 Sustain changes.			Knowledge transfer plans	BAI08.02; BAI08.03
			Communications of management's commitment	Internal
			Reviews of operational use	MEA02.02
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 change management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.7. Business Change Management
Change implementation planning and management	Skills Framework for the Information Age V6, 2015	CIPM
Organization design and implementation	Skills Framework for the Information Age V6, 2015	ORDI

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Organizational change management policy	Provides framework and outlines principles for managing organizational change. Reflects current legislation and provides good people-management practices; ensures consistent approach to managing change across the organization.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Realizing value from I&T-enabled investments requires more than delivering I&T solutions and services. It also requires changes to business processes, skills and competencies, culture and behavior, etc., all of which must be included in the business case for the investment. Leadership must create a culture of continuous change through flexibility, openness and confidence and establish appropriate change management support and communication.		

G. Component: Services, Infrastructure and Applications
• Communication tools and channels • Surveying tools

Domain: Build, Acquire and Implement Management Objective: BAI06 — Managed IT Changes	Focus Area: COBIT Core Model

Description

Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritization and authorization, emergency changes, tracking, reporting, closure, and documentation.

Purpose

Enable fast and reliable delivery of change to the business. Mitigate the risk of negatively impacting the stability or integrity of the changed environment.

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	AG06 Agility to turn business requirements into operational solutions
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	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

A. Component: Process

Management Practice	Example Metrics
BAI06.01 Evaluate, prioritize and authorize change requests. Evaluate all requests for change to determine the impact on business processes and I&T services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled.	a. Amount of rework caused by failed changes b. Percent of unsuccessful changes due to inadequate impact assessments

Activities	Capability Level
1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.	2
2. Categorize all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.	
3. Prioritize all requested changes based on the business and technical requirements; resources required; and the legal, regulatory and contractual reasons for the requested change.	
4. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.	
5. Plan and schedule all approved changes.	
6. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, privacy, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies among changes. Involve business process owners in the assessment process, as appropriate.	3
7. Consider the impact of contracted services providers (e.g., of outsourced business processing, infrastructure, application development and shared services) on the change management process. Include integration of organizational change management processes with change management processes of service providers and the impact on contractual terms and SLAs.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SY2.4 Change Management
ISO/IEC 20000-1:2011(E)	9.2 Change management
ITIL V3, 2011	Service Transition, 4.2 Change Management
PMBOK Guide Sixth Edition, 2017	Part 1: 4.6 Perform Integrated Change Control

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI06.02 Manage emergency changes. Carefully manage emergency changes to minimize further incidents. Ensure the emergency change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorized after the change.	a. Number of emergency changes not authorized after the incident b. Percent of total changes that are emergency fixes
Activities	**Capability Level**
1. Define what constitutes an emergency change.	2
2. Ensure that a documented procedure exists to declare, assess, approve preliminarily, authorize after the change and record an emergency change.	
3. Verify that all emergency access arrangements for changes are appropriately authorized, documented and revoked after the change has been applied.	3
4. Monitor all emergency changes and conduct post-implementation reviews involving all concerned parties. The review should consider and initiate corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI06.03 Track and report change status. Maintain a tracking and reporting system to document rejected changes and communicate the status of approved, in-process and complete changes. Make certain that approved changes are implemented as planned.	a. Number and age of backlogged change requests b. Percent of change request status reported to stakeholders in a timely manner
Activities	**Capability Level**
1. Categorize change requests in the tracking process (e.g., rejected, approved but not yet initiated, approved and in process, and closed).	4
2. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g., aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition.	
3. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.	
4. Maintain a tracking and reporting system for all change requests.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.CC Apply Change Control
Management Practice	**Example Metrics**
BAI06.04 Close and document the changes. Whenever changes are implemented, update the solution, user documentation and procedures affected by the change.	a. Number of review errors found in the documentation b. Percent of user documentation and procedures updates performed in a timely manner
Activities	**Capability Level**
1. Include changes in the documentation within the management procedure. Examples of documentation include business and IT operational procedures, business continuity and disaster recovery documentation, configuration information, application documentation, help screens, and training materials.	2
2. Define an appropriate retention period for change documentation and pre- and post-change system and user documentation.	3
3. Subject documentation to the same level of review as the actual change.	
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	Business Process Owners	Program Manager	Project Manager	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritize and authorize change requests.	A	R			R	R	R	R	R	R
BAI06.02 Manage emergency changes.	A				R	R	R	R		R
BAI06.03 Track and report change status.	A	R	R	R	R	R	R			
BAI06.04 Close and document the changes.	A	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
BAI06.01 Evaluate, prioritize and authorize change requests.	BAI03.05	Integrated and configured solution components	Change plan and schedule	BAI07.01
	DSS02.03	Approved service requests	Approved requests for change	BAI07.01
	DSS03.03	Proposed solutions to known errors	Impact assessments	Internal
	DSS03.05	Identified sustainable solutions		
	DSS04.08	Approved changes to the plans		
	DSS06.01	Root cause analyses and recommendations		
BAI06.02 Manage emergency changes.			Post-implementation review of emergency changes	Internal
BAI06.03 Track and report change status.	BAI03.09	Record of all approved and applied change requests	Change request status reports	BAI01.06; BAI10.03
BAI06.04 Close and document the changes.			Change documentation	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**
Change management	Skills Framework for the Information Age V6, 2015	CHMG
Change support	e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	C. Run - C.2. Change Support

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**
Leaders must create a culture of continuous improvement in IT solutions and services, recognizing that improvement requires them to understand the impact of technology change on the enterprise, its inherent risk and associated mitigation, as well as its cost. Leaders must balance the impact of change against its expected benefits and contribution to I&T strategy and enterprise objectives.		

G. Component: Services, Infrastructure and Applications
• Configuration management tools • IT change management tools

Domain: Build, Acquire and Implement Management Objective: BAI07 — Managed IT Change Acceptance and Transitioning	Focus Area: COBIT Core Model

Description

Formally accept and make operational new solutions. Include implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and I&T services, early production support, and a post-implementation review.

Purpose

Implement solutions safely and in line with the agreed expectations and outcomes.

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	AG06 Agility to turn business requirements into operational solutions
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	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

A. Component: Process

Management Practice	Example Metrics
BAI07.01 Establish an implementation plan. Establish an implementation plan that covers system and data conversion, acceptance testing criteria, communication, training, release preparation, promotion to production, early production support, a fallback/back-up plan, and a post-implementation review. Obtain approval from relevant parties.	a. Number and category of stakeholders signing off on the implementation plan b. Number of implementation plans that are robust and contain all required components

Activities	Capability Level
1. Create an implementation plan that reflects the broad implementation strategy, the sequence of implementation steps, resource requirements, inter-dependencies, criteria for management acceptance of the production implementation, installation verification requirements, transition strategy for production support, and update of business continuity plans.	2
2. From external solution providers, obtain commitment to their involvement in each step of the implementation.	
3. Identify and document the fallback and recovery processes.	
4. Confirm that all implementation plans are approved by technical and business stakeholders and reviewed by internal audit, as appropriate.	3
5. Formally review the technical and business risk associated with implementation. Ensure that the key risk is considered and addressed in the planning process.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Transition, 4.1 Transition Planning and Support

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI07.02 Plan business process, system and data conversion. Prepare for business process, I&T service data and infrastructure migration as part of the enterprise's development methods. Include audit trails and a recovery plan should the migration fail.	a. Percent of successful conversion b. Percent of necessary adjustments made to procedures (including revised roles and responsibilities and control procedures)

Activities	Capability Level
1. Define a business process, I&T service data and infrastructure migration plan. In developing the plan, consider, for example, hardware, networks, operating systems, software, transaction data, master files, backups and archives, interfaces with other systems (both internal and external), possible compliance requirements, business procedures, and system documentation.	2
2. In the business process conversion plan, consider all necessary adjustments to procedures, including revised roles and responsibilities and control procedures.	
3. Confirm that the data conversion plan does not require changes in data values unless absolutely necessary for business reasons. Document changes made to data values, and secure approval from the business process data owner.	
4. Plan retention of backup and archived data to conform to business needs and regulatory or compliance requirements.	
5. Rehearse and test the conversion before attempting a live conversion.	
6. Coordinate and verify the timing and completeness of the conversion cutover so there is a smooth, continuous transition with no loss of transaction data. Where necessary, in the absence of any other alternative, freeze live operations.	
7. Plan to back up all systems and data taken at the point prior to conversion. Maintain audit trails to enable the conversion to be retraced. Ensure that there is a recovery plan that covers rollback of migration and fallback to previous processing should the migration fail.	
8. In the data conversion plan, incorporate methods for collecting, converting and verifying data to be converted, and identifying and resolving any errors found during conversion. Include comparing the original and converted data for completeness and integrity.	3
9. Consider the risk of conversion problems, business continuity planning and fallback procedures in the business process, data and infrastructure migration plan where there are risk management, business needs or regulatory/compliance requirements.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Transition, 4.1 Transition Planning and Support

Management Practice	Example Metrics
BAI07.03 Plan acceptance tests. Establish a test plan based on enterprisewide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.	a. Percent of stakeholders satisfied with the completeness of testing process b. Number of documented test plans that include all testing phases and robust testing scenarios and are appropriate to the operational requirements and environment

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Develop and document the test plan, which aligns to the program, project quality plan and relevant organizational standards. Communicate and consult with appropriate business process owners and IT stakeholders.	2
2. Ensure that the test plan reflects an assessment of risk from the project and that all functional and technical requirements are tested. Based on assessment of the risk of system failure and faults on implementation, include in the plan requirements for performance, stress, usability, pilot, security testing and privacy.	
3. Ensure that the test plan addresses the potential need for internal or external accreditation of outcomes of the test process (e.g., financial or regulatory requirements).	
4. Ensure that the test plan identifies necessary resources to execute testing and evaluate the results. Examples of resources may be construction of test environments and use of staff time for the test group, including potential temporary replacement of test staff in the production or development environments. Ensure that stakeholders are consulted on the resource implications of the test plan.	
5. Ensure that the test plan identifies testing phases appropriate to the operational requirements and environment. Examples of such testing phases include unit test, system test, integration test, user acceptance test, performance test, stress test, data conversion test, security test, privacy test, operational readiness test, and backup and recovery tests.	
6. Confirm that the test plan considers test preparation (including site preparation), training requirements, installation or an update of a defined test environment, planning/performing/documenting/retaining test cases, error and problem handling, correction and escalation, and formal approval.	
7. Confirm that all test plans are approved by stakeholders, including business process owners and IT, as appropriate. Stakeholders may include application development managers, project managers and business process end users.	
8. Ensure that the test plan establishes clear criteria for measuring the success of undertaking each testing phase. Consult the business process owners and IT stakeholders in defining the success criteria. Determine that the plan establishes remediation procedures when the success criteria are not met. For example, if there is a significant failure in a testing phase, the plan should provide guidance on whether to proceed to the next phase, stop testing or postpone implementation.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
BAI07.04 Establish a test environment. Define and establish a secure test environment representative of the planned business process and IT operations environment in terms of performance, capacity, security, internal controls, operational practices, data quality, privacy requirements and workloads.	a. Level of comparability between test environment and future business and operational landscape b. Level of sanitized test data (and/or databases) that are representative of the production environment
Activities	**Capability Level**
1. Create a database of test data that are representative of the production environment. Sanitize data used in the test environment from the production environment according to business needs and organizational standards. For example, consider whether compliance or regulatory requirements oblige the use of sanitized data.	2
2. Protect sensitive test data and results against disclosure, including access, retention, storage and destruction. Consider the effect of interaction of organizational systems with those of third parties.	3
3. Put in place a process to enable proper retention or disposal of test results, media and other associated documentation that will enable adequate review and subsequent analysis or efficient retesting as required by the test plan. Consider the effect of regulatory or compliance requirements.	
4. Ensure that the test environment is representative of the future business and operational landscape. Include business process procedures and roles, likely workload stress, operating systems, necessary application software, database management systems, and network and computing infrastructure found in the production environment.	
5. Ensure that the test environment is secure and incapable of interacting with production systems.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI07.05 Perform acceptance tests. Test changes independently, in accordance with the defined test plan, prior to migration to the live operational environment.	a. Number of identified gaps between acceptance test results and the defined success criteria b. Number of successful acceptance tests

Activities	Capability Level
1. Review the categorized log of errors found in the testing process by the development team. Verify that all errors have been remediated or formally accepted.	2
2. Evaluate the final acceptance against the success criteria and interpret the final acceptance testing results. Present them in a form that is understandable to business process owners and IT, so an informed review and evaluation can take place.	3
3. Approve the acceptance, with formal sign-off by the business process owners, third parties (as appropriate) and IT stakeholders prior to promotion.	
4. Ensure that testing of changes is undertaken in accordance with the testing plan. Ensure that the testing is designed and conducted by a test group that is independent from the development team. Consider the extent to which business process owners and end users are involved in the test group. Ensure that testing is conducted only within the test environment.	
5. Ensure that the tests and anticipated outcomes are in accordance with the defined success criteria set out in the testing plan.	
6. Consider using clearly defined test instructions (scripts) to implement the tests. Ensure that the independent test group assesses and approves each test script to confirm that it adequately addresses test success criteria set out in the test plan. Consider using scripts to verify the extent to which the system meets security and privacy requirements.	
7. Consider the appropriate balance between automated scripted tests and interactive user testing.	
8. Undertake tests of security in accordance with the test plan. Measure the extent of security weaknesses or loopholes. Consider the effect of security incidents since construction of the test plan. Consider the effect on access and boundary controls. Consider privacy.	
9. Undertake tests of system and application performance in accordance with the test plan. Consider a range of performance metrics (e.g., end-user response times and database management system update performance).	
10. When undertaking testing, ensure that the fallback and rollback elements of the test plan have been addressed.	
11. Identify, log and classify (e.g., minor, significant, mission-critical) errors during testing. Ensure that an audit trail of test results is available. In accordance with the test plan, communicate results of testing to stakeholders to facilitate bug fixing and further quality enhancement.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Transition, 4.5 Service Validation and Testing

Management Practice	Example Metrics
BAI07.06 Promote to production and manage releases. Promote the accepted solution to the business and operations. Where appropriate, run the solution as a pilot implementation or in parallel with the old solution for a defined period and compare behavior and results. If significant problems occur, revert to the original environment based on the fallback/back-up plan. Manage releases of solution components.	a. Number and percent of releases not ready for release on schedule b. Percent of stakeholder satisfaction with the implemented solution

Activities	Capability Level
1. Prepare for transfer of business procedures and supporting services, applications and infrastructure from testing to the production environment in accordance with organizational change management standards.	2
2. Determine the extent of pilot implementation or parallel processing of the old and new systems in line with the implementation plan.	
3. Promptly update relevant business process and system documentation, configuration information and contingency plan documents, as appropriate.	
4. Ensure that all media libraries are updated promptly with the version of the solution component being transferred from testing to the production environment. Archive the existing version and its supporting documentation. Ensure that promotion to production of systems, application software and infrastructure is under configuration control.	
5. Where distribution of solution components is conducted electronically, control automated distribution to ensure that users are notified, and distribution occurs only to authorized and correctly identified destinations. In the release process, include backup procedures to enable the distribution of changes to be reviewed in the event of a malfunction or error.	
6. Where distribution takes physical form, keep a formal log of what items have been distributed, to whom, where they have been implemented, and when each has been updated.	