Domain: Evaluate, Direct and Monitor Governance Objective: EDM05 — Ensured Stakeholder Engagement	Focus Area: COBIT Core Model

Description

Ensure that stakeholders are identified and engaged in the I&T governance system and that enterprise I&T performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and necessary remedial actions.

Purpose

Ensure that stakeholders are supportive of the I&T strategy and road map, communication to stakeholders is effective and timely, and the basis for reporting is established to increase performance. Identify areas for improvement, and confirm that I&T-related objectives and strategies are in line with the enterprise's strategy.

The governance 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

Governance Practice	Example Metrics
EDM05.01 Evaluate stakeholder engagement and reporting requirements. Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	a. Date of last revision to reporting requirements b. Percent of stakeholders covered in reporting requirements

Activities	Capability Level
1. Identify all relevant I&T stakeholders within and outside the enterprise. Group stakeholders in stakeholder categories with similar requirements.	2
2. Examine and make judgment on the current and future mandatory reporting requirements relating to the use of I&T within the enterprise (regulation, legislation, common law, contractual), including extent and frequency.	
3. Examine and make judgment on the current and future communication and reporting requirements for other stakeholders relating to the use of I&T within the enterprise, including required level of involvement/consultation and extent of communication/level of detail and conditions.	
4. Maintain principles for communication with external and internal stakeholders, including communication formats and channels, and for stakeholder acceptance and sign-off of reporting.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	SR.DR Direct Stakeholder Communication and Reporting

A. Component: Process *(cont.)*	
Governance Practice	**Example Metrics**
EDM05.02 Direct stakeholder engagement, communication and reporting. Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting, and creating a communication strategy for stakeholders.	a. Number of breaches of mandatory reporting requirements b. Stakeholder satisfaction with communication and reporting

Activities	Capability Level
1. Direct the establishment of the consultation and communication strategy for external and internal stakeholders.	2
2. Direct the implementation of mechanisms to ensure that information meets all criteria for mandatory I&T reporting requirements for the enterprise.	
3. Establish mechanisms for validation and approval of mandatory reporting.	
4. Establish reporting escalation mechanisms.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	SR.AR Apply Stakeholder Reporting Requirements
King IV Report on Corporate Governance for South Africa, 2016	Part 5.5: Stakeholder relationships—Principle 16
King IV Report on Corporate Governance for South Africa, 2016	Part 5.2: Strategy, performance and reporting—Principle 5
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity V1.1, April 2018	3.3 Communicating Cybersecurity Requirements with Stakeholders

Governance Practice	Example Metrics
EDM05.03 Monitor stakeholder engagement. Monitor stakeholder engagement levels and the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders in terms of reporting and communication are met.	a. Level of stakeholder engagement with enterprise I&T b. Percent of reports containing inaccuracies c. Percent of reports delivered on time

Activities	Capability Level
1. Periodically assess the effectiveness of the mechanisms for ensuring the accuracy and reliability of mandatory reporting.	4
2. Periodically assess the effectiveness of the mechanisms for, and outcomes from, involvement of and communication with external and internal stakeholders.	
3. Determine whether the requirements of different stakeholders are met and assess stakeholder engagement levels.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	SR.MC Monitor Stakeholder Communication

B. Component: Organizational Structures					
Key Governance Practice	**Board**	**Executive Committee**	**Chief Executive Officer**	**Chief Risk Officer**	**Chief Information Officer**
EDM05.01 Evaluate stakeholder engagement and reporting requirements.	A	R	R	R	R
EDM05.02 Direct stakeholder engagement communication and reporting.	A	R	R	R	R
EDM05.03 Monitor stakeholder engagement.	A	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance

C. Component: Information Flows and Items (see also Section 3.6)				
Governance Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
EDM05.01 Evaluate stakeholder engagement and reporting requirements.	EDM02.04	Actions to improve value delivery	Reporting and communications principles	MEA01.01
	EDM03.03	Risk management issues for the board	Evaluation of enterprise reporting requirements	MEA01.01
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities		
EDM05.02 Direct stakeholder engagement, communication and reporting.	APO12.04	Risk analysis and risk profile reports for stakeholders	Rules for validating and approving mandatory reports	MEA01.01; MEA03.04
			Escalation guidelines	MEA01.05
EDM05.03 Monitor stakeholder engagement.	MEA04.08	• Assurance review results • Assurance review report	Assessment of reporting effectiveness	MEA01.01; MEA03.04

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

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
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

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Transparency policy	Addresses the importance of frequent, open communication with all stakeholders to ensure that they understand the strategic importance of I&T to enterprise success. Ensures that transparency supports appropriate risk mitigation, linking transparency and effective risk management to I&T value and enterprise growth.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Create a culture in which open and structured communication is provided to key stakeholders, in line with their requirements.		

G. Component: Services, Infrastructure and Applications
• Communication tools and channels • IT dashboarding • Stakeholder survey tools

Domain: Align, Plan and Organize Management Objective: APO06 — Managed Budget and Costs	Focus Area: COBIT Core Model

Description

Manage the I&T-related financial activities in both the business and IT functions, covering budget, cost and benefit management and prioritization of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the I&T strategic and tactical plans. Initiate corrective action where needed.

Purpose

Foster a partnership between IT and enterprise stakeholders to enable the effective and efficient use of I&T-related resources and provide transparency and accountability of the cost and business value of solutions and services. Enable the enterprise to make informed decisions regarding the use of I&T solutions and services.

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 • EG09 Optimization of business process costs • EG12 Managed digital transformation programs	• AG04 Quality of technology-related financial information • 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	AG04	a. Satisfaction of key stakeholders regarding the level of transparency, understanding and accuracy of I&T financial information b. Percent of I&T services with defined and approved operational costs and expected benefits
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	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
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		
EG09	a. Ratio of cost vs. achieved service levels b. Satisfaction levels of board and executive management with business processing costs		
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**
APO06.01 Manage finance and accounting. Establish and maintain a method to manage and account for all I&T-related costs, investments and depreciation as an integral part of enterprise financial systems and accounts. Report using the enterprise's financial measurement systems.	a. Numbers of deviations between expected and actual budget categories b. Usefulness of financial information as input to business cases for new investment in I&T assets and services

Activities	Capability Level
1. Define processes, inputs, outputs and responsibilities for the financial management and accounting of I&T in alignment with the enterprise budgeting and cost accounting policies and approach. Define how to analyze and report (to whom and how) on the I&T budget control process.	2
2. Define a classification scheme to identify all I&T-related cost elements (capital expenditures [capex] vs. operational expenses [opex], hardware, software, people, etc.). Identify how they are captured.	
3. Use financial information to provide input to business cases for new investments in I&T assets and services.	3
4. Ensure that costs are maintained in the I&T assets and services portfolios.	
5. Establish and maintain practices for financial planning and the optimization of recurring operational costs to deliver maximum value to the enterprise for the least expenditure.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service Strategy, 4.3 Financial management for IT services

Management Practice	Example Metrics
APO06.02 Prioritize resource allocation. Implement a decision-making process to prioritize the allocation of resources and establish rules for discretionary investments by individual business units. Include the potential use of external service providers and consider the buy, develop and rent options.	a. Number of resource-allocation issues escalated b. Percent of alignment of I&T resources with high-priority initiatives

Activities	Capability Level
1. Rank all I&T initiatives and budget requests based on business cases and strategic and tactical priorities. Establish procedures to determine budget allocations and cutoff.	2
2. Allocate business and IT resources (including external service providers) within the high-level budget allocations for I&T-enabled programs, services and assets. Consider the options for buying or developing capitalized assets and services vs. externally utilized assets and services on a pay-for-use basis.	
3. Establish a procedure to communicate budget decisions and review them with the business unit budget holders.	
4. Identify, communicate and resolve significant impacts of budget decisions on business cases, portfolios and strategy plans. For example, this may include when budgets require revision due to changing enterprise circumstances or when they are not sufficient to support strategic objectives or business case objectives).	
5. Obtain ratification from the executive committee for the I&T budget implications that negatively impact the entity's strategic or tactical plans. Suggest actions to resolve these impacts.	3

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

Management Practice	Example Metrics
APO06.03 Create and maintain budgets. Prepare a budget reflecting investment priorities based on the portfolio of I&T-enabled programs and I&T services.	a. Number of budget changes due to omissions and errors b. Usefulness of I&T budget in identifying all expected I&T costs of I&T-enabled programs, services and assets

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Implement a formal I&T budget, including all expected I&T costs of I&T-enabled programs, services and assets.	2
2. When creating the budget, consider the following components: alignment with the business; alignment with the sourcing strategy; authorized sources of funding; internal resource costs, including personnel, information assets and accommodations; third-party costs, including outsourcing contracts, consultants and service providers; capital and operational expenses; and cost elements that depend on the workload.	
3. Document the rationale to justify contingencies and review them regularly.	
4. Instruct process, service and program owners, as well as project and asset managers, to plan budgets.	
5. Review the budget plans and make decisions about budget allocations. Compile and adjust the budget based on changing enterprise needs and financial considerations.	3
6. Record, maintain and communicate the current I&T budget, including committed expenditures and current expenditures, considering I&T projects recorded in the I&T-enabled investment portfolios and operation and maintenance of asset and service portfolios.	
7. Monitor the effectiveness of the different aspects of budgeting.	4
8. Use the monitoring results to implement improvements and ensure that future budgets are more accurate, reliable and cost-effective.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 20000-1:2011(E)	6.4 Budgeting and accounting for services
PMBOK Guide Sixth Edition, 2017	Part 1: 7. Project cost management

Management Practice	Example Metrics
APO06.04 Model and allocate costs. Establish and use an I&T costing model based, for example, on the service definition. This approach ensures that allocation of costs for services is identifiable, measurable and predictable, and encourages the responsible use of resources, including those provided by service providers. Regularly review and benchmark the cost/chargeback model to maintain its relevance and appropriateness for evolving business and IT activities.	a. Percent of overall I&T costs that are allocated according to the agreed cost models b. Number of reviews and benchmarks of the cost/chargeback model and its appropriateness to evolving business and I&T activities

Activities	Capability Level
1. Decide on a cost allocation model that enables fair, transparent, repeatable and comparable allocation of I&T-related costs to users. A basic allocation model example is the even spread of shared I&T-related costs. This is a very simple allocation model that is easy to apply; however, depending on the context of the enterprise, it is often viewed as unfair and it does not encourage responsible use of resources. An activity-based costing scheme, in which costs are allocated to IT services and charged to users of these services, enables a more transparent and comparable allocation of cost.	3
2. Inspect service definition catalogs to identify services subject to user chargeback and those that are shared services.	
3. Design the cost model to be transparent enough to allow users to identify their actual usage and charges by using categories and cost drivers that make sense for the user (e.g., cost per help desk call, cost per software license) and to better enable predictability of I&T costs and efficient and effective utilization of I&T resources. Analyze cost drivers (time spent per activity, expenses, portion of fixed vs. variable costs, etc.). Decide on appropriate differentiation (e.g., different categories of users with different weights) and use cost approximations or averages when actual costs are highly variable in nature.	
4. Explain the cost model principles and outcome to key stakeholders. Obtain their feedback for further fine-tuning toward a transparent and comprehensive model.	
5. Obtain approval of key stakeholders and communicate the I&T costing model to the management of user departments.	
6. Communicate important changes in the cost/chargeback model principles to key stakeholders and management of user departments.	

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

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO06.05 Manage costs. Implement a cost management process that compares actual costs against budget. Costs should be monitored and reported. Deviations from budget should be identified in a timely manner and their impact on enterprise processes and services assessed.	a. Percent of variance among budgets, forecasts and actual costs b. Timeliness of monitoring and reporting in the case of deviations and the impact of deviations on enterprise processes and services assessed

Activities	Capability Level
1. Obtain approval of key stakeholders and communicate the I&T costing model to the management of user departments.	2
2. Establish time scales for the operation of the cost management process in line with budgeting and accounting requirements and timeline.	
3. Define a method for the collection of relevant data to identify deviations in budget vs. actuals, investment ROI, service cost trends, etc.	
4. Define how costs are consolidated for the appropriate levels in the enterprise (central IT vs. IT budget within business departments) and how they will be presented to the stakeholders. The reports provide information on costs per cost category, budget vs. actuals status, top spending, etc., to enable the timely identification of required corrective actions.	3
5. Instruct those responsible for cost management to capture, collect and consolidate the data, and present and report the data to the appropriate budget owners. Budget analysts and owners jointly analyze deviations and compare performance to internal and industry benchmarks. They should establish and maintain the overheads allocation method. The result of the analysis provides an explanation of significant deviations and the suggested corrective actions.	
6. Ensure that the appropriate levels of management review the results of the analysis and approve suggested corrective actions.	
7. Ensure that changes in cost structures and enterprise needs are identified and budgets and forecasts are revised as required.	4
8. At regular intervals, and especially when budgets are cut due to financial constraints, identify ways to optimize costs and introduce efficiencies without jeopardizing services.	5

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

B. Component: Organizational Structures						
Key Management Practice	**Chief Financial Officer**	**Chief Information Officer**	**Chief Technology Officer**	**Chief Digital Officer**	**Portfolio Manager**	**Head IT Administration**
APO06.01 Manage finance and accounting.	A				R	R
APO06.02 Prioritize resource allocation.	R	A	R	R	R	R
APO06.03 Create and maintain budgets.	R	A	R	R		R
APO06.04 Model and allocate costs.	R	A				R
APO06.05 Manage costs.	R	A	R	R		R

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

C. Component: Management Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
APO06.01 Manage finance and accounting.	**From**	**Description**	**Description**	**To**
	BAI09.01	Asset register	Financial planning practices	Internal
			I&T costs classification scheme	Internal
			Accounting processes	Internal
APO06.02 Prioritize resource allocation.	APO04.04	Proof-of-concept scope and outline business case	Budget allocations	APO02.05; APO05.02; APO07.05; BAI03.11
	APO05.01	Investment return expectations	Prioritization and ranking of I&T initiatives	APO05.02
	APO05.02	• Program business case • Business case assessments		
	EDM02.02	Evaluation of investment and services portfolios		
	EDM02.04	Actions to improve value delivery		
APO06.03 Create and maintain budgets.			I&T budget	APO02.05; APO05.02; APO07.01; BAI03.11
			Budget communications	APO05.02; APO07.01; BAI03.11
APO06.04 Model and allocate costs.			Operational procedures	Internal
			Cost allocation communications	Internal
			Cost allocation model	Internal
			Categorized I&T costs	Internal
APO06.05 Manage costs.	BAI01.02	Program benefit realization plan	Cost optimization opportunities	APO02.02
	BAI01.04	Program budget and benefits register	Cost consolidation method	Internal
	BAI01.05	Results of benefit realization monitoring	Cost data collection method	Internal
	EDM02.04	Feedback on portfolio and program performance		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 7. Project cost management: Inputs and Outputs

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

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Budgeting policy	Addresses preparation and timeline for the annual budget and forecasting of the annual financial position. Outlines required management reporting processes. Establishes accountability and responsibility for budget plan and other financial documents.		

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Effective and efficient management of I&T is supported by a culture of transparency on budget, costs and benefits throughout the organization. Management should enable a culture of fact-based decision-making through, for example, comparable estimations of business and IT costs and benefits for input to portfolio management, fair cost allocation of IT assets and resources, and repeatable budgeting of IT budgets.		

G. Component: Services, Infrastructure and Applications
Cost accounting system

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

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**	
BAI02.01 Define and maintain business functional and technical requirements.	**From**	**Description**	**Description**	**To**
	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

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

Description

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

Purpose

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Component: Organizational Structures

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

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

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

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

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

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

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

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

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

Description

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

Purpose

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

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

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

Example Metrics for Enterprise Goals		Example Metrics for Alignment Goals	
EG01	a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05	a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG02	a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG07	a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment
EG06	a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets		
EG08	a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities		

A. Component: Process	
Management Practice	**Example Metrics**
DSS04.01 Define the business continuity policy, objectives and scope. Define business continuity policy and scope, aligned with enterprise and stakeholder objectives, to improve business resilience.	a. Percent of business continuity objectives and scope reworked due to misidentified processes and activities b. Percent of key stakeholders participating, defining and agreeing on continuity policy and scope

Activities	Capability Level
1. Identify internal and outsourced business processes and service activities that are critical to the enterprise operations or necessary to meet legal and/or contractual obligations.	2
2. Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.	
3. Define and document the agreed minimum policy objectives and scope for business resilience.	
4. Identify essential supporting business processes and related I&T services.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
HITRUST CSF version 9, September 2017	12.01 Information Security Aspects of Business Continuity Management
ISF, The Standard of Good Practice for Information Security 2016	BC1.1 Business Continuity Strategy; BC1.2 Business Continuity Programme
ISO/IEC 27002:2013/Cor.2:2015(E)	17. Information security aspects of business continuity management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-1)

Management Practice	Example Metrics
DSS04.02 Maintain business resilience. Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption.	a. Total downtime resulting from major incident or disruption b. Percent of key stakeholders involved in business impact analyses evaluating the impact over time of a disruption to critical business functions and the effect that a disruption would have on them

Activities	Capability Level
1. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.	2
2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.	
3. Establish the minimum time required to recover a business process and supporting I&T, based on an acceptable length of business interruption and maximum tolerable outage.	
4. Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.	
5. Assess the likelihood of threats that could cause loss of business continuity. Identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.	3
6. Analyze continuity requirements to identify possible strategic business and technical options.	
7. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.	
8. Obtain executive business approval for selected strategic options.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	BC1.3 Resilient Technical Environments
ITIL V3, 2011	Service Design, 4.6 IT Continuity Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-2)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
DSS04.01 Define the business continuity policy, objectives and scope.	**From**	**Description**	**Description**	**To**
	APO09.03	SLAs	Policy and objectives for business continuity	APO01.02
			Assessments of current continuity capabilities and gaps	Internal
			Disruptive incident scenarios	Internal
DSS04.02 Maintain business resilience.	APO12.06	• Risk impact communication • Risk-related root causes	Approved strategic options	APO02.05
			BIAs	APO12.02
			Continuity requirements	Internal
DSS04.03 Develop and implement a business continuity response.	APO09.03	OLAs	Incident response actions and communications	DSS02.01
			BCP	Internal
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).			Test results and recommendations	Internal
			Test exercises	Internal
			Test objectives	Internal
DSS04.05 Review, maintain and improve the continuity plans.			Recommended changes to plans	Internal
			Results of reviews of plans	Internal
DSS04.06 Conduct continuity plan training.	HR	List of personnel requiring training	Monitoring results of skills and competencies	APO07.03
			Training requirements	APO07.03
DSS04.07 Manage backup arrangements.	APO14.10	• Backup plan • Backup test plan	Test results of backup data	Internal
			Backup data	Internal; APO14.08
DSS04.08 Conduct post-resumption review.			Approved changes to the plans	BAI06.01
			Post-resumption review report	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this component				

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

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

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

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

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

Description

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

Purpose

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

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

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

A. Component: Process

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

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

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

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

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

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

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

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

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

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

B. Component: Organizational Structures

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

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

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

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

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

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

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

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