Domain: Evaluate, Direct and Monitor **Governance Objective: EDM03 — Ensured Risk Optimization**		**Focus Area: COBIT Core Model**
Description		
Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of I&T is identified and managed.		
Purpose		
Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.		
The governance objective supports the achievement of a set of primary enterprise and alignment goals:		
Enterprise Goals	➡	**Alignment Goals**
• EG02 Managed business risk • EG06 Business service continuity and availability		• AG02 Managed I&T-related risk • AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals		**Example Metrics for Alignment Goals**
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile		AG02 a. Frequency of updating risk profile b. Percent of enterprise risk assessments including I&T-related risk c. Number of significant I&T-related incidents that were not identified in a risk assessment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets		AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment

A. Component: Process	
Governance Practice	**Example Metrics**
EDM03.01 Evaluate risk management. Continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.	a. Level of unexpected enterprise impact b. Percent of I&T risk that exceeds enterprise risk tolerance c. Refreshment rate of risk factor evaluation
Activities	**Capability Level**
1. Understand the organization and its context related to I&T risk.	2
2. Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.	
3. Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.	
4. Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.	
5. Proactively evaluate I&T risk factors in advance of pending strategic enterprise decisions and ensure that risk considerations are part of the strategic enterprise decision process.	3
6. Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.	
7. Attract and maintain necessary skills and personnel for I&T Risk Management	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16

Evaluate, Direct and Monitor

A. Component: Process *(cont.)*	
Governance Practice	**Example Metrics**
EDM03.02 Direct risk management. Direct the establishment of risk management practices to provide reasonable assurance that I&T risk management practices are appropriate and that actual I&T risk does not exceed the board's risk appetite.	a. Level of alignment between I&T risk and enterprise risk b. Percent of enterprise projects that consider I&T risk
Activities	**Capability Level**
1. Direct the translation and integration of the I&T risk strategy into risk management practices and operational activities.	2
2. Direct the development of risk communication plans (covering all levels of the enterprise).	
3. Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).	
4. Direct that risk, opportunities, issues and concerns may be identified and reported by anyone to the appropriate party at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.	
5. Identify key goals and metrics of the risk governance and management processes to be monitored, and approve the approaches, methods, techniques and processes for capturing and reporting the measurement information.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RS.AS Apply Risk Management Strategy; BC.RO Determine Strategic Risk Objectives
ISF, The Standard of Good Practice for Information Security 2016	IR1.1 Information Risk Assessment—Management Approach
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas—Principle 11
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.5 Assessment (Task 2)
Governance Practice	**Example Metrics**
EDM03.03 Monitor risk management. Monitor the key goals and metrics of the risk management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	a. Number of potential I&T risk areas identified and managed b. Percent of critical risk that has been effectively mitigated c. Percent of I&T risk action plans executed on time
Activities	**Capability Level**
1. Report any risk management issues to the board or executive committee.	2
2. Monitor the extent to which the risk profile is managed within the enterprise's risk appetite and tolerance thresholds.	3
3. Monitor key goals and metrics of risk governance and management processes against targets, analyze the cause of any deviations, and initiate remedial actions to address the underlying causes.	4
4. Enable key stakeholders' review of the enterprise's progress toward identified goals.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	9. Review and Revision—Principle 17
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7); 3.5 Assessment (Task 1); 3.6 Authorization (Task 1)
The Open Group IT4IT Reference Architecture, Version 2.0	6. Requirement to Deploy (R2D) Value Stream; 7. Request to Fulfill (R2F) Value Stream

B. Component: Organizational Structures								
Key Governance Practice	**Board**	**Executive Committee**	**Chief Executive Officer**	**Chief Risk Officer**	**Chief Information Officer**	**I&T Governance Board**	**Enterprise Risk Committee**	**Chief Information Security Officer**
EDM03.01 Evaluate risk management.	A	R	R	R	R	R	R	
EDM03.02 Direct risk management.	A	R	R	R	R	R	R	
EDM03.03 Monitor risk management.	A	R	R	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle
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**
EDM03.01 Evaluate risk management.	APO12.01	Emerging risk issues and factors	Risk appetite guidance	APO04.01; APO12.03
	Outside COBIT	Enterprise risk management (ERM) principles	Evaluation of risk management activities	APO12.01
			Approved risk tolerance levels	APO12.03
EDM03.02 Direct risk management.	APO12.03	Aggregated risk profile, including status of risk management actions	Approved process for measuring risk management	APO12.01
	Outside COBIT	Enterprise risk management (ERM) profiles and mitigation plans	Key objectives to be monitored for risk management	APO12.01
			Risk management policies	APO12.01
EDM03.03 Monitor risk management.	APO12.02	Risk analysis results	Remedial actions to address risk management deviations	APO12.06
	APO12.04	• Risk analysis and risk profile reports for stakeholders • Results of third-party risk assessments • Opportunities for acceptance of greater risk	Risk management issues for the board	EDM05.01

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.5 Assessment (Tasks 1, 2): Inputs 2, and Outputs; 3.6 Authorization (Task 1): Inputs and Outputs

D. Component: People, Skills and Competencies

Skill	Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Business risk management	Skills Framework for the Information Age V6, 2015	BURM
Risk management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Component: Policies and Procedures

Relevant Policy	Policy Description	Related Guidance	Detailed Reference
Enterprise risk policy	Defines governance and management of enterprise risk at strategic, tactical and operational levels, pursuant to business objectives. Translates enterprise governance into risk governance principles and policy and elaborates risk management activities.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-1)

F. Component: Culture, Ethics and Behavior

Key Culture Elements	Related Guidance	Detailed Reference
Promote an I&T risk-aware culture at all levels of the organization and empower the enterprise proactively to identify, report and escalate I&T risk, opportunity and potential business impacts. Senior management sets direction and demonstrates visible and genuine support for risk practices. Additionally, management must clearly define risk appetite and ensure an appropriate level of debate as part of business-as-usual activities. Desirable behaviors include encouraging employees to raise issues or negative outcomes and show transparency with regard to I&T risk. Business owners should accept ownership of I&T risk when applicable and demonstrate genuine commitment to I&T risk management by providing adequate resource levels.	COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principles 3 and 4

G. Component: Services, Infrastructure and Applications

G. Component: Services, Infrastructure and Applications
Risk management system

Align, Plan and Organize

Domain: Align, Plan and Organize Management Objective: APO13 — Managed Security	Focus Area: COBIT Core Model
Description	
Define, operate and monitor an information security management system.	
Purpose	
Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.	
The management objective supports the achievement of a set of primary enterprise and alignment goals:	

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

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

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

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	0.01 Information Security Management program
ISO/IEC 20000-1:2011(E)	6.6 Information security management
ITIL V3, 2011	Service Design, 4.7 Information Security Management
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 1); 3.4 Implementation (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-2)
Management Practice	**Example Metrics**
APO13.02 Define and manage an information security and privacy risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases, implemented as an integral part of services and solutions development, and operated as an integral part of business operation.	a. Percentage of successful security risk scenario simulations b. Number of employees who have successfully completed information security awareness training
Activities	**Capability Level**
1. Formulate and maintain an information security risk treatment plan aligned with strategic objectives and the enterprise architecture. Ensure that the plan identifies the appropriate and optimal management practices and security solutions, with associated resources, responsibilities and priorities for managing identified information security risk.	3
2. Maintain as part of the enterprise architecture an inventory of solution components that are in place to manage security-related risk.	
3. Develop proposals to implement the information security risk treatment plan, supported by suitable business cases that include consideration of funding and allocation of roles and responsibilities.	
4. Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan.	
5. Implement information security and privacy training and awareness programs.	
6. Integrate the planning, design, implementation and monitoring of information security and privacy procedures and other controls capable of enabling prompt prevention, detection of security events, and response to security incidents.	
7. Define how to measure the effectiveness of the selected management practices. Specify how these measurements are to be used to assess effectiveness to produce comparable and reproducible results.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
APO13.03 Monitor and review the information security management system (ISMS). Maintain and regularly communicate the need for, and benefits of, continuous improvement in information security. Collect and analyze data about the information security management system (ISMS), and improve its effectiveness. Correct nonconformities to prevent recurrence.	a. Frequency of scheduled security reviews b. Number of findings in regularly scheduled security reviews c. Level of stakeholder satisfaction with the security plan d. Number of security-related incidents caused by failure to adhere to the security plan

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

B. Component: Organizational Structures

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

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

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

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

Align, Plan and Organize

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

Management Practice	Inputs		Outputs	
	From	**Description**	**Description**	**To**
APO13.03 Monitor and review the information security management system (ISMS).	DSS02.02	Classified and prioritized incidents and service requests	Recommendations for improving the information security management system (ISMS)	Internal
			Information security management system (ISMS) audit reports	MEA02.01

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.3 Selection (Tasks 1, 3): Inputs and Outputs; 3.4 Implementation (Task 1): Inputs and Outputs

D. Component: People, Skills and Competencies

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

E. Component: Policies and Procedures

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

F. Component: Culture, Ethics and Behavior

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

G. Component: Services, Infrastructure and Applications

- Configuration management tools
- Security and privacy awareness services
- Third-party security assessment services

Domain: Build, Acquire and Implement Management Objective: BAI04 — Managed Availability and Capacity	Focus Area: COBIT Core Model
Description	
Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.	
Purpose	
Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.	
The management objective supports the achievement of a set of primary enterprise and alignment goals:	

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

A. Component: Process

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

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

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

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
BAI04.02 Assess business impact. Identify important services to the enterprise. Map services and resources to business processes and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. For vital business functions, ensure that availability requirements can be satisfied per service level agreement (SLA).	a. Number of scenarios created to assess future availability situations b. Percent of business process owners signing off on analysis results
Activities	**Capability Level**
1. Identify only those solutions or services that are critical in the availability and capacity management process.	2
2. Map the selected solutions or services to the application(s) and infrastructure (IT and facility) on which they depend to enable a focus on critical resources for availability planning.	3
3. Collect data on availability patterns from logs of past failures and performance monitoring. Use modeling tools that help predict failures based on past usage trends and management expectations of new environment or user conditions.	4
4. Based on the collected data, create scenarios that describe future availability situations to illustrate a variety of potential capacity levels needed to achieve the availability performance objective.	
5. Based on the scenarios, determine the likelihood that the availability performance objective will not be achieved.	
6. Determine the impact of the scenarios on the business performance measures (e.g., revenue, profit, customer services). Engage the business-line, functional (especially finance) and regional leaders to understand their evaluation of impact.	
7. Ensure that business process owners fully understand and agree to the results of this analysis. From the business owners, obtain a list of unacceptable risk scenarios that require a response to reduce risk to acceptable levels.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	6.3 Service continuity and availability management
Management Practice	**Example Metrics**
BAI04.03 Plan for new or changed service requirements. Plan and prioritize availability, performance and capacity implications of changing business needs and service requirements.	a. Number of unplanned capacity, performance or availability upgrades b. Percent that management performs comparisons of actual demand on resources against forecasted supply and demand
Activities	**Capability Level**
1. Identify availability and capacity implications of changing business needs and improvement opportunities. Use modeling techniques to validate availability, performance and capacity plans.	3
2. Review availability and capacity implications of service trend analysis.	4
3. Ensure that management performs comparisons of actual demand on resources against forecasted supply and demand to evaluate current forecasting techniques and make improvements where possible.	
4. Prioritize needed improvements and create cost-justifiable availability and capacity plans.	5
5. Adjust the performance and capacity plans and SLAs based on realistic, new, proposed and/or projected business processes and supporting services, applications and infrastructure changes. Also include reviews of actual performance and capacity usage, including workload levels.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	5. Design and transition of new changed services
Management Practice	**Example Metrics**
BAI04.04 Monitor and review availability and capacity. Monitor, measure, analyze, report and review availability, performance and capacity. Identify deviations from established baselines. Review trend analysis reports identifying any significant issues and variances. Initiate actions where necessary and ensure that all outstanding issues are addressed.	a. Number of events exceeding planned limits for capacity b. Number of transaction peaks exceeding target performance

A. Component: Process *(cont.)*	
Activities	**Capability Level**
1. Provide capacity reports to the budgeting processes.	2
2. Establish a process for gathering data to provide management with monitoring and reporting information for availability, performance and capacity workload of all I&T-related resources.	3
3. Provide regular reporting of the results in an appropriate form for review by IT and business management and communication to enterprise management.	4
4. Integrate monitoring and reporting activities in the iterative capacity management activities (monitoring, analysis, tuning and implementations).	

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

Management Practice	**Example Metrics**
BAI04.05 Investigate and address availability, performance and capacity issues. Address deviations by investigating and resolving identified availability, performance and capacity issues.	a. Number and percentage of unresolved availability, performance and capacity issues b. Number of availability incidents

Activities	**Capability Level**
1. Obtain guidance from vendor product manuals to ensure an appropriate level of performance availability for peak processing and workloads.	3
2. Define an escalation procedure for swift resolution in case of emergency capacity and performance problems.	
3. Identify performance and capacity gaps based on monitoring current and forecasted performance. Use the known availability, continuity and recovery specifications to classify resources and allow prioritization.	4
4. Define corrective actions (e.g., shifting workload, prioritizing tasks or adding resources when performance and capacity issues are identified).	5
5. Integrate required corrective actions into the appropriate planning and change management processes.	

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

B. Component: Organizational Structures

Key Management Practice	**Executive Committe**	**Chief Information Officer**	**Chief Technology Officer**	**Business Process Owners**	**Head Architect**	**Head IT Operations**	**Service Manager**	**Business Continuity Manager**
BAI04.01 Assess current availability, performance and capacity and create a baseline.		R	A	R		R	R	
BAI04.02 Assess business impact.	A			R		R	R	
BAI04.03 Plan for new or changed service requirements.		R	A	R		R	R	
BAI04.04 Monitor and review availability and capacity.	A			R		R	R	
BAI04.05 Investigate and address availability, performance and capacity issues.		R	A	R	R	R	R	R

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

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

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI04.01 Assess current availability, performance and capacity and create a baseline.	BAI02.01	Requirements definition repository	Evaluations against SLAs	APO09.05
	BAI02.03	Requirements risk register	Availability, performance and capacity baselines	Internal
BAI04.02 Assess business impact.	BAI03.02	Internal and external service level agreements (SLAs)	Availability, performance and capacity business impact assessments	Internal
			Availability, performance and capacity scenarios	Internal
BAI04.03 Plan for new or changed service requirements.	BAI02.01	Confirmed acceptance criteria from stakeholders	Performance and capacity plans	APO02.02
	BAI03.01	Approved high-level design specification	Prioritized improvements	APO02.02
	BAI03.02	Approved detailed design specification		
	BAI03.03	Documented solution components		
BAI04.04 Monitor and review availability and capacity.			Availability, performance and capacity monitoring review reports	MEA01.03
BAI04.05 Investigate and address availability, performance and capacity issues.			Corrective actions	APO02.02
			Emergency escalation procedure	DSS02.02
			Performance and capacity gaps	Internal

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

D. Component: People, Skills and Competencies

Skill	Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Availability management	Skills Framework for the Information Age V6, 2015	AVMT
Capacity management	Skills Framework for the Information Age V6, 2015	CPMG

E. Component: Policies and Procedures

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

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

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

Domain: Deliver, Service and Support Management Objective: DSS05 - Managed Security Services		Focus Area: COBIT Core Model
Description		
Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges. Perform security monitoring.		
Purpose		
Minimize the business impact of operational information security vulnerabilities and incidents.		
The management objective supports the achievement of a set of primary enterprise and alignment goals:		
Enterprise Goals	➡	**Alignment Goals**
• EG02 Managed business risk • EG06 Business service continuity and availability		• AG02 Managed I&T-related risk • AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals		**Example Metrics for Alignment Goals**
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile		AG02 a. Frequency of updating risk profile b. Percent of enterprise risk assessments including I&T-related risk c. Number of significant I&T-related incidents that were not identified in a risk assessment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets		AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment

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

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

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

A. Component: Process *(cont.)*

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

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

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

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

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

Deliver, Service and Support

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

A. Component: Process *(cont.)*

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

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

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

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

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

A. Component: Process *(cont.)*

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	CM.Ph Monitor Physical
HITRUST CSF version 9, September 2017	01.06 Application & Information Access Control; 01.07 Mobile Computing & Teleworking; 08.0 Physical & Environmental Security; 10.03 Cryptographic Controls; 10.04 Security of System Files
ISF, The Standard of Good Practice for Information Security 2016	IR2.3 Business Impact Assessment - Confidentiality Requirements; IR2.4 Business Impact Assessment - Integrity Requirements; IR2.5 Business Impact Assessment - Availability Requirements; IM2.2 Sensitive Physical Information; PA2.2 Enterprise Mobility Man
ISO/IEC 27002:2013/Cor.2:2015(E)	10. Cryptography
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.1 Access control (AC-2, AC-3, AC-4, AC-5, AC-6, AC-13, AC-24); 3.7 Identification and authentication (IA-2, IA-10, IA-11)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 15: Wireless Access Control

Management Practice	Example Metrics
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events. Using a portfolio of tools and technologies (e.g., intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	a. Number of vulnerability tests carried out on perimeter devices b. Number of vulnerabilities discovered during testing c. Time taken to remediate any vulnerabilities d. Percent of tickets created in a timely manner when monitoring systems identify potential security incidents

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

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

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

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

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
DSS05.01 Protect against malicious software.	**From**	**Description**	**Description**	**To**
			Malicious software prevention policy	APO01.02
			Evaluations of potential threats	APO12.02; APO12.03
DSS05.02 Manage network and connectivity security.	APO01.07	Data classification guidelines	Connectivity security policy	APO01.02
	APO09.03	SLAs	Results of penetration tests	MEA04.07
DSS05.03 Manage endpoint security.	APO03.02	Information architecture model	Security policies for endpoint devices	APO01.02
	APO09.03	• SLAs • OLAs		
	BAI09.01	Results of physical inventory checks		
	DSS06.06	Reports of violations		
DSS05.04 Manage user identity and logical access.	APO01.05	Definition of I&T-related roles and responsibilities	Results of reviews of user accounts and privileges	Internal
	APO03.02	Information architecture model	Approved user access rights	Internal

Deliver, Service and Support

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

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Information security	Skills Framework for the Information Age V6, 2015	SCTY
Information security management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage— E.8. Information Security Management
Penetration testing	Skills Framework for the Information Age V6, 2015	PENT
Security administration	Skills Framework for the Information Age V6, 2015	SCAD

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

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

G. Component: Services, Infrastructure and Applications

- Directory services
- Email filtering systems
- Identity and access management system
- Security awareness services
- Security information and event management (SIEM) tools
- Security operations center (SOC) services
- Third-party security assessment services
- URL filtering systems

Domain: Monitor, Evaluate and Assess Management Objective: MEA03 — Managed Compliance With External Requirements			Focus Area: COBIT Core Model
Description			
Evaluate that I&T processes and I&T-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with; integrate IT compliance with overall enterprise compliance.			
Purpose			
Ensure that the enterprise is compliant with all applicable external requirements.			
The management objective supports the achievement of a set of primary enterprise and alignment goals:			
Enterprise Goals	➡	**Alignment Goals**	
EG03 Compliance with external laws and regulations		AG01 I&T compliance and support for business compliance with external laws and regulations	
Example Metrics for Enterprise Goals		**Example Metrics for Alignment Goals**	
EG03 a. Cost of regulatory noncompliance, including settlements and fines b. Number of regulatory noncompliance issues causing public comment or negative publicity c. Number of noncompliance matters noted by regulators d. Number of regulatory noncompliance issues relating to contractual agreements with business partners		AG01 a. Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss b. Number of IT-related noncompliance issues reported to the board, or causing public comment or embarrassment c. Number of noncompliance issues relating to contractual agreements with IT service providers	

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

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

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

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
MEA03.02 Optimize response to external requirements. Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider adopting and adapting industry standards, codes of good practice, and good practice guidance.	a. Average time between identifying external compliance issues and resolution b. Percent of satisfaction of relevant personnel with communication of new and changed regulatory compliance requirements
Activities	**Capability Level**
1. Regularly review and adjust policies, principles, standards, procedures and methodologies for their effectiveness in ensuring necessary compliance and addressing enterprise risk. Use internal and external experts, as required.	3
2. Communicate new and changed requirements to all relevant personnel.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas - Principle 13
Management Practice	**Example Metrics**
MEA03.03 Confirm external compliance. Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements.	a. Number of critical noncompliance issues identified per year b. Percent of process owners signing off, confirming compliance
Activities	**Capability Level**
1. Regularly evaluate organizational policies, standards, procedures and methodologies in all functions of the enterprise to ensure compliance with relevant legal and regulatory requirements in relation to the processing of information.	3
2. Address compliance gaps in policies, standards and procedures on a timely basis.	
3. Periodically evaluate business and IT processes and activities to ensure adherence to applicable legal, regulatory and contractual requirements.	
4. Regularly review for recurring patterns of compliance failures and assess lessons learned.	4
5. Based on review and lessons learned, improve policies, standards, procedures, methodologies, and associated processes and activities.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Metrics**
MEA03.04 Obtain assurance of external compliance. Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.	a. Number of compliance reports obtained b. Percent of service provider compliance based on independent reviews c. Time between identification of compliance gap and corrective action d. Number of corrective action reports addressing compliance gaps closed in a timely manner
Activities	**Capability Level**
1. Obtain regular confirmation of compliance with internal policies from business and IT process owners and unit heads.	2
2. Perform regular (and, where appropriate, independent) internal and external reviews to assess levels of compliance.	
3. If required, obtain assertions from third-party I&T service providers on levels of their compliance with applicable laws and regulations.	
4. If required, obtain assertions from business partners on levels of their compliance with applicable laws and regulations as they relate to intercompany electronic transactions.	
5. Integrate reporting on legal, regulatory and contractual requirements at an enterprisewide level, involving all business units.	3
6. Monitor and report on noncompliance issues and, where necessary, investigate the root cause.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Quality Assurance
ISO/IEC 27002:2013/Cor.2:2015(E)	18. Compliance

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

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

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
MEA03.01 Identify external compliance requirements.	Outside COBIT	Legal and regulatory compliance requirements	Log of required compliance actions	Internal
			Compliance requirements register	Internal

MEA03.02 Optimize response to external requirements.			Communications of changed compliance requirements	All APO;
				All BAI;
				All DSS;
				All MEA;
				EDM01.01

			Updated policies, principles, procedures and standards	APO01.09; APO01.11
MEA03.03 Confirm external compliance.	BAI05.06	Compliance audit results	Compliance confirmations	EDM01.03
	BAI09.05	Results of installed license audits	Identified compliance gaps	MEA04.08
	BAI10.05	License deviations		
	DSS01.04	Insurance policy reports		
MEA03.04 Obtain assurance of external compliance.	EDM05.02	Rules for validating and approving mandatory reports	Compliance assurance reports	EDM01.03
	EDM05.03	Assessment of reporting effectiveness	Reports of noncompliance issues and root causes	EDM01.03; MEA04.04

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

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

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

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

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