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	
	From	Description	Description	To
DSS04.01 Define the business continuity policy, objectives and scope.	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