CERT® Resilience Management Model v1.1

Crosswalk of NIST Special Publications

CERT® RESILIENCE MANAGEMENT MODEL V1.1	NIST SPECIAL PUBLICATIONS											
PROCESS AREA GOALS AND PRACTICES	800-18 REV.1	800-30	800-34 REV. 1	800-37	800-39	800-53	800-53A	800-55 REV. 1	800-60 VOL. 1 REV.1	800-61 REV. 1	800-70 REV. 2	800-137
ADM – ASSET DEFINITION AND MANAGEMENT												
ADM:SG1 Establish Organizational Assets	1.7			2.3	2.6.2	CM, PE, PL-2, PM-5, PL-4, RA-2	3.1		3.1			2.4
ADM:SG2 Establish the Relationship Between Assets and Services				2.1, 2.3		PM-11, RA-2						
ADM:SG3 Manage Assets												2.1.1
AM – ACCESS MANAGEMENT												
AM:SG1 Manage and Control Access						AC-1, AC-2, AC-10, IA-1, IA-2, IA-8, MA-3, MA-4, MA-5, PE-1, PE-7, PE-16, PL-2, SA-7, SC-2, SI-9, SI-11						
COMM – COMMUNICATIONS												
COMM:SG1 Prepare for Resilience Communications										2.4.4, 2.3.4		2.1, 3.1.1
COMM:SG2 Prepare for Communications Management							3.1					2.1.3
COMM:SG3 Deliver Resilience Communications			4.2.2				3.1					
COMM:SG4 Improve Communications												
COMP – COMPLIANCE												
COMP:SG1 Prepare for Compliance Management						CA-1, AU-1, AU-3, AU-5						2.2
COMP:SG2 Establish Compliance Obligations						AU-2, SI-4, AU-1						2.2, 2.4
COMP:SG3 Demonstrate Satisfaction of Compliance Obligations						AU-6, AU-11, PL-6						2.2, 3.1.2
COMP:SG4 Monitor Compliance Activities												
CTRL – CONTROLS MANAGEMENT												
CTRL:SG1 Establish Control Objectives			3.4	2.4			3.1, 3.2.1					2.3, 3.1.2
CTRL:SG2 Establish Controls			3.4	2.4, Task 2-1, Task 2-2		PM-7						3.1.2
CTRL:SG3: Analyze Controls				Task 2-1, Task 2-3, Task 3-1, Appendix G			3.2.1, 3.2.2					2.2, 3.1.1
CTRL:SG4 Assess Control Effectiveness				Task 4-1, Task 4-2, Task 4-3, Task 4-4, Task 6-2, Task 6-3			3.3					2.2, 3.1.2, 3.5.1
EC – ENVIRONMENTAL CONTROL												
EC:SG1 Establish and Prioritize Facility Assets			3.4.3									
EC:SG2 Protect Facility Assets			3.4.3			PE-3, PE-4, PE-6, PE-7, PE-8, PE-9, PE-13, PE-16, PE-17, PE-18	3.1				3	
EC:SG3 Manage Facility Asset Risk						PM-4, PM-7						3.1.2, 3.6
EC:SG4 Control Operational Environment			3.2			CP-6, CP-7, CP-8, PE-10, PE-11, PE-12, PE-13, PM-11, PE-14, PE-15			3.2, 4.6			
EF – ENTERPRISE FOCUS												
EF:SG1 Establish Strategic Objectives			3.2.1			PM-7, PM-11	3.1	1.4, 5.2, 5.5.2				2.1
EF:SG2 Plan for Operational Resilience						PL-2, PM-1, PM-4						
EF:SG3 Establish Sponsorship						PL-1, PM-3	3.1					
EF:SG4 Provide Resilience Oversight						CA-6, PL-1, PL-2, PM-6		6.3				3.3.2
EXD – EXTERNAL DEPENDENCIES												
EXD:SG1 Identify and Prioritize External Dependencies												
EXD:SG2 Manage Risks Due to External Dependencies												3.1.2, 3.6
EXD:SG3 Establish Formal Relationships						AC-20, CA-3, SA-2, SA-3, SA-9, SA-11, SA-12, SA-13						
EXD:SG4 Manage External Entity Performance						SA-3, SA-9, SA-12, SA-13						
FRM – FINANCIAL RESOURCE MANAGEMENT												
FRM:SG1 Establish Financial Commitment												
FRM:SG2 Perform Financial Planning												
FRM:SG3 Fund Resilience Activities			3.4.5									
FRM:SG4 Account for Resilience Activities												2.3
FRM:SG5 Optimize Resilience Expenditures and Investments												
HRM – HUMAN RESOURCE MANAGEMENT												
HRM:SG1 Establish Resource Needs							3.1			2.4.2		
HRM:SG2 Manage Staff Acquisition						PE-2	3.1					
HRM:SG3 Manage Staff Performance							3.1					
HRM:SG4 Manage Changes to Employment Status												
ID – IDENTITY MANAGEMENT												
ID:SG1 Establish Identities						AC-5, AC-6, AC-22, IA-2, IA-4, PE-2						2.4
ID:SG2 Manage Identities						AC-2						
IMC – INCIDENT MANAGEMENT AND CONTROL												
IMC:SG1 Establish the Incident Management and Control Process						AC-14, IR-2, IR-4, IR-8				2.3		
IMC:SG2 Detect Events			4.2			IR-4, IR-5, IR-6, IR-7, PE-6, SI-5				3.2, 3.3.2, 3.4.3, 4.3, 4.4.2, 5.3, 5.4.2, 6.3, 6.4.2, 7.3, 8.2		2.1.3
IMC:SG3 Declare Incidents			4.2.1, 4.2.3			IR-4				3.2.4, 4.3, 5.3, 6.3, 7.3, 8.2		3.1.1, 3.3.4,
IMC:SG4 Respond to and Recover from Incidents			4.2.2			IR-4				2.3.4, 3, 4, 5, 6, 7, 8		2.1.3, 3.3.4
IMC:SG5 Establish Incident Learning										3.4		3.3.4

CERT® RESILIENCE MANAGEMENT MODEL V1.1	NIST SPECIAL PUBLICATIONS											
PROCESS AREA GOALS AND PRACTICES	800-18 REV.1	800-30	800-34 REV. 1	800-37	800-39	800-53	800-53A	800-55 REV. 1	800-60 VOL. 1 REV.1	800-61 REV. 1	800-70 REV. 2	800-137
KIM – KNOWLEDGE AND INFORMATION MANAGEMENT												
KIM:SG1 Establish and Prioritize Information Assets				2.1		AC-22			3.1.1, 4			
KIM:SG2 Protect Information Assets			3.4.1, 3.4.2			AC-16, AC-21, PE-5, SC-2, SI-12	3.1		3.1.2, 4			
KIM:SG3 Manage Information Asset Risk		3, 4, 5				PM-4, PM-7	PM-7					3.1.2, 3.6
KIM:SG4 Manage Information Asset Confidentiality and Privacy						AU-13, IA-1, MP-2, MP-3, MP-4, MP-5, MP-6, PL-5, SC-8, SC-9, SC-11, SC-12, SC-13, SC-14, SC-17, SI-12						
KIM:SG5 Manage Information Asset Integrity						SC-8, SC-14, SC-20, SC-21						2.1.1
KIM:SG6 Manage Information Asset Availability						CP-9				3.4.3		
MA – MEASUREMENT AND ANALYSIS												
MA:SG1 Align Measurement and Analysis Activities						PM-6	3.1, 3.2.1, 3.2.2, Appendix D, Appendix F	3.4.3, 3.4.4, 5.2, 5.5, 5.7, 6.1		3.2.4, 3.4.3, 4.3, 5.3, 6.3, 7.3, 8.2		2.1.2, 2.1.3, 3.1.1, 3.1.3, 3.2
MA:SG2 Provide Measurement Results							3.3, Appendix G	3.4.3, 6.2				2.1.3, 3.4, 3.5
MON – MONITORING												
MON:SG1 Establish and Maintain a Monitoring Program						CA-7, PM-6, SI-4		5.1, 5.2			3	2.1, 2.3, 3.1, 3.3, 3.5
MON:SG2 Perform Monitoring					3.4	RA-5, SI-4		6.1, 6.2				2.1.3, 2.2, 2.3, 3.3, 3.4, 3.5.2
OPD – ORGANIZATIONAL PROCESS DEFINITION												
OPD:SG1 Establish Organizational Process Assets						PM-11	3.2, Appx. D, Appendix E			3, 4, 5, 6, 7, 8		3.1.1
OPF – ORGANIZATIONAL PROCESS FOCUS												
OPF:SG1 Determine Process Improvement Opportunities							3.2.5					2.3, 3.1.1, 3.7
OPF:SG2 Plan and Implement Process Actions							3.2.5					3.7
OPF:SG3 Deploy Organizational Process Assets and Incorporate Experiences												3.1.1, 3.7
OTA – ORGANIZATIONAL TRAINING AND AWARENESS												
OTA:SG1 Establish Awareness Program						AT-1						
OTA:SG2 Conduct Awareness Activities						AT-2				3.2.3		3.1.1
OTA:SG3 Establish Training Capability			3.5			AT-1						
OTA:SG4 Conduct Training						AT-3, AT-4						
PM – PEOPLE MANAGEMENT												
PM:SG1 Establish Vital Staff										2.4.3		
PM:SG2 Manage Risks Associated with Staff Availability						PM-4, PM-7				2.4.3		
PM:SG3 Manage the Availability of Staff						PM-11						
RISK – RISK MANAGEMENT												
RISK:SG1 Prepare for Risk Management		2, 3.2		2.1	2.1, 2.2, 2.6, 3.2	PM-9, RA-2	3.1			3.1.2, 4.2.2, 5.2.2, 6.2.2, 7.2.2		2.1.3, 2.2, 3.1.1
RISK:SG2 Establish Risk Parameters and Focus		3.7			2.2, 3.2	CA-6, PM-9, RA-3	3.1	5.5				2.1.3, 2.2, 3.1.1
RISK:SG3 Identify Risk		3			3.2	CA-2, PL-5, PL-6, PM-9, RA-3			4.2, 4.3, 4.4, 4.5			2.2
RISK:SG4 Analyze Risk		3, 5		2.1		PL-5, PL-6, PM-9, RA-3						2.2, 3.1.1
RISK:SG5 Mitigate and Control Risk		4			2.2	CA-5, PM-4, PM-9, RA-3						3.1.2, 3.6
RISK:SG6 Use Risk Information to Manage Resilience						PM-9						2.2, 3.1.1
RRD – RESILIENCE REQUIREMENTS DEVELOPMENT												
RRD:SG1 Identify Enterprise Requirements						PM-7	2.3					
RRD:SG2 Develop Service Requirements	1.8, 2					SA-2, SA-13, PM-7	2.3, 3.1, 3.2.1		4.6		3	
RRD:SG3 Analyze and Validate Requirements	3.9					SA-13	3.1				4	2.1
RRM – RESILIENCE REQUIREMENTS MANAGEMENT												
RRM:SG1 Manage Requirements	2.5, 3					PM-7, SA-2	3.1		4.6			2.1.1, 2.1.2, 3.6, 3.7
RTSE – RESILIENT TECHNICAL SOLUTION MANAGEMENT												
RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development				2.2		SA-4, SA-11, SA-13					3	
RTSE:SG2 Develop Resilient Technical Solution Development Plans	2.4			2.2		SSA-3, A-12, SA-14, PM-7					4	
RTSE:SG3 Execute the Plan						SA-12, SA-14						2.2
SC – SERVICE CONTINUITY												
SC:SG1 Prepare for Service Continuity			3.1, 3.4, 4			CP-1, PM-11						
SC:SG2 Identify and Prioritize High-Value Services			3.2			AT-5, CP-2, PM-8, SC-8, SC-9						
SC:SG3 Develop Service Continuity Plans			3.4, 3.5.2			CP-2, CP-3, CP-10, PL-6, PM-11						
SC:SG4 Validate Service Continuity Plans												
SC:SG5 Exercise Service Continuity Plans			3.5.3			CP-3, CP-4, PL-6						
SC:SG6 Execute Service Continuity Plans												
SC:SG7 Maintain Service Continuity Plans			3.6			CP-2						
TM – TECHNOLOGY MANAGEMENT												
TM:SG1 Establish and Prioritize Technology Assets			3.2.3			PL-2, PM-5, SA-14						
TM:SG2 Protect Technology Assets	2.5, 3.2, 3.13, 3.14		3.3			AC-14, AU-3, AU-7, AU-8, AU-9, AU-10, AU-12, AU-14, CM-6, CM-7, PA-5, PL-2, PL-6, PM-7, SA-13, SC-2	3.1		3.1, 4		3	
TM:SG3 Manage Technology Asset Risk		3, 5	3.3			CM-4, PL-6, PM-4, PM-7, PM-10						3.1.2, 3.6
TM:SG4 Manage Technology Asset Integrity	2.5, 3.13, 3.14, 3.16					AC-3, AC-4, AC-7, AC-8, AC-9, AC-11, AC-17, AC-18, AC-19, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-9, IA-2, IA-3, IA-5, IA-6, IA-7, IA-8, MA-1, MA-3, MA-4, MA-5, PM-10, SA-5, SA-10, SI-2, SI-5						2.1.1, 2.1.2, 2.2
TM:SG5 Manage Technology Asset Availability	3.11		3.4.4			AU-4, AU-5, MA-2, MA-4, MA-6, PE-11, PL-6, PM-11, SI-6, SI-13						
VAR – VULNERABILITY ANALYSIS AND RESOLUTION												
VAR:SG1 Prepare for Vulnerability Analysis and Resolution		3.3					2.2, 2.3, 3.2, Appendix D, Appendix E			4.2.2, 5.2.2, 6.2.2, 7.2.2	3	3.1.1
VAR:SG2 Identify and Analyze Vulnerabilities		3.3.1, 3.3.2, 3.4, 3.6	3.3			RA-5, SA-10, SA-11, SI-2, SI-3				3.1.2, 3.2.4		2.1.2, 2.1.3, 3.1.2
VAR:SG3 Manage Exposure to Vulnerabilities			3.3			RA-5, SA-10, SA-11, SI-2, SI-3						
VAR:SG4 Identify Root Causes						RA-5, SA-11, SI-2				3.4		

NO WARRANTY
THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.
Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.
This document may not be reproduced without permission. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.
This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a
royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

The referenced special publications were developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. National Institute of Standards and Technology. U.S. Department of Commerce. Computer Security Division. Information Technology Laboratory, Gaithersburg, MD.

© 2011 Carnegie Mellon University