OMB Control No. 1670-NEW

Expiration Date: XX/XX/XXXX

Draft Nationwide Cyber Security Review Question Set

The Nationwide Cyber Security Review (NCSR) is a VOLUNTARY survey.

Paperwork Reduction Act
The public reporting burden to complete this information collection is estimated at two (2) hours or less per respondent, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the assessment questions. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/National Protection and Programs Directorate, Michael Leking, 703-235-3030, Michael.Leking@dhs.gov, ATTN: PRA [*OMB Control Number: 1670-NEW*].

Privacy Act Statement
Authority: Title XVIII of the Homeland Security Act of 2002, 6 U.S.C. § 101 et seq., and the Implementing Recommendations of the 9/11 Commission Act or 2007 (6 U.S.C. 579(m) authorizes the collection of this information.
Purpose: The primary purpose of this assessment is to examine relationships, interactions, and processes governing IT management and the ability to effectively manage operational risk within States and Large Urban Areas.
Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/All-003 Department of Homeland Security General Training Records (November 25, 2008, 73 FR 228).

This report was prepared for the United States Department of Homeland Security

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official U.S. Government or U.S. Agency (including, but not limited to DoD or DHS) position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Homeland Security. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2011 Carnegie Mellon University.

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 report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use. This document may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created with the funding and support of the U.S. Department of Homeland Security under the Federal Government Contract Number FA8721-05-C-0003 between the U.S. Department of Defense and 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. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this page.

Process Area	Question	Range of potential answers for the Respondent to select.				
ADM	**Does your organization identify and document information about the people who are vital to the continued operation of high-value services, including those it does not directly employ?**	No	People who are vital to high-value services are identified informally, but their roles or functions in support of those services are not documented	An asset management database or other repository identifies and describes the roles of internal employees who are vital to high-value services, but not contracted or other external staff	Yes, a repository identifies all vital staff and describes their roles in support of high-value services	
ADM	**Does your organization identify and inventory the information, technology, and facility assets that directly support the continued operation of high-value services?**	No	Some leased or owned assets are inventoried	All leased or owned assets are inventoried	Most or all information, technology, and facility assets are inventoried, but they are not tracked by which services they support	Yes, all information, technology, and facility assets that directly support high-value services are inventoried. including those that are not directly controlled
ADM	**In your inventory of high-value assets (people, information, technology, and facilities), is there a standard or template that helps ensure consistency among asset descriptions?**	No, or no such inventory exists	For one or two asset types only	Yes, descriptions of like or similar assets are consistent	Yes, descriptions are consistent and are communicated to those who need to know	
ADM	**Are both owners and custodians of high-value assets identified and documented in asset descriptions in the asset inventory?**	No, or no such asset descriptions exist	Owners of assets, but not custodians	Yes, both owners and custodians		
ADM	**If an asset supports more than one high-value service, are dependencies**	No	Dependencies and potential conflicts are	Yes, dependencies and potential conflicts are	Yes, and mitigation plans are developed	

and potential conflicts identified, and are they analyzed as to how they might affect the operational resilience of the associated services?	identified as risks but are not further analyzed	identified and analyzed	and implemented to reduce the effects of conflicts or, if possible, to reduce or eliminate the conflicts themselves

ADM	**Has your organization established a set of criteria for changes in assets or their associations with services that trigger required updates of the asset inventory, including updates of related resilience requirements?**	No, or no inventory exists	Yes, for some assets	Yes, for all assets	Yes, for all assets, and the criteria are related to the organization's resilience requirements		
ADM	**Do you update asset descriptions and other relevant documents (such as protection strategies and continuity plans) whenever changes are made to high-value assets?**	No	Asset descriptions for most assets are updated, but not other documents	Yes, asset descriptions and other relevant documents are updated	Yes, using a change control process that includes keeping a change history that shows the rationale for performing changes	Yes, using a change control process, and custodians are notified of changes that affect them	Yes, using a change control process, and the impact of asset changes on existing resilience requirements and activities is evaluated
ADM	**Does your organization document the associations between assets and the high-value services they support?**	No, or high-value services have not been identified	Such associations are generally known within organizational units but are not documented	Yes, for some asset types or in some organizational units	Yes, all high-value asset-service associations are identified and documented		
COMP	**Have guidelines and standards for satisfying compliance obligations been established and communicated?**	No	They are established and communicated at the individual organizational unit or line of business level but are not coordinated across the organization	Yes, they are established and communicated as part of the enterprise-level compliance program			
COMP	**Is the organization's compliance process monitored, evaluated, and improved?**	No	Through self-assessment, with limited follow-through for improvement	Through self-assessment, with extensive follow-through for improvement	Through independent evaluation, with extensive follow-through for improvement		
COMP	**Does your organization develop, implement, and track plans to address**	Areas needing remediation are not	Areas needing remediation are	Yes, remediation plans are developed,			

areas in which remediation is needed to satisfy compliance obligations?	consistently identified	identified, but there is no formal process to address them	implemented, and tracked to completion

COMP	**Does your organization track progress against schedules for compliance obligations and identify obligations that may not be met?**	No	Yes, for all external governmental, regulatory, and industry compliance obligations	Yes, for both external obligations and internal standards and policies where applicable		
COMP	**Has your organization implemented processes for data validation and integrity checking to ensure that compliance data is accurate, complete, and timely?**	No	For very few compliance obligations (<10%)	For some compliance obligations (10%–50%)	For many compliance obligations (>50% but <100%)	Yes, for all compliance obligations
COMP	**Does your organization have documented strategies for the collection of compliance data?**	No	No, but there are established procedures for data collection	Yes, there are documented strategies for ensuring that all data needed to satisfy obligations is collected	Yes, and the strategies address issues related to the data collection, storage, and retrieval infrastructure	
COMP	**Are specific compliance obligations assigned to specific owners?**	No	Very few (<10%)	Some (10%–50%)	Many (>50% but <100%)	Yes (100%)
COMP	**Are compliance obligations identified and documented?**	No	There is an informal inventory of compliance obligations	There is a formal, documented inventory for at least one type of obligation (e.g., human resources directives)	Yes, formally documented for numerous types of obligations	
COMP	**Does your organization have a compliance program to carry out the activities and practices of the compliance strategic plan?**	No, or there is no compliance plan	Compliance activities are conducted at the individual organizational unit or line of business level but are not coordinated across the organization	Yes	Yes, and sponsorship and oversight of the compliance program are provided	
COMP	**Does your organization develop a plan for managing compliance obligations**	No	Plans, resources, and sponsorship are	Yes, a plan is developed at the enterprise level,	Yes, and the plan and commitments	

as part of its strategic planning process?	developed at the organizational unit or line of business level but are not coordinated across the organization	and commitments are obtained	are revised on a cycle aligned with the organization's strategic planning process

COMP	**Are compliance obligations analyzed and organized to facilitate satisfaction?**	No	Some compliance obligations or types of obligations	Yes, most compliance obligations	Yes, and any conflicting obligations are identified and documented	
CTRL	**Has your organization done a baseline analysis of existing controls against control objectives to identify gaps where control objectives are not adequately satisfied?**	No, or control objectives are not defined	For some control objectives, if a problem is evident	For most control objectives, as part of a routine process	Yes, for all control objectives, as part of an established process at levels commensurate with their importance in sustaining operational resilience	
CTRL	**Are control objectives defined and documented to guide the selection, implementation, and management of controls?**	No	In very few organizational units (<10%)	In some organizational units (10%–50%)	In many organizational units (>50% but <100%)	Yes, in all organizational units (100%)
CTRL	**Does your organization assess controls periodically to verify that they are continuing to meet control objectives and satisfy resilience requirements?**	No	Controls are reassessed only after they are modified	Some controls are assessed periodically	All service- and asset-level controls are assessed periodically	All controls, including enterprise-level controls, are assessed periodically as part of an established process
CTRL	**Does your organization identify and implement enterprise-level controls to protect services and assets from disruption?**	No	Only the minimum needed to meet regulatory requirements	A few types of enterprise-level controls are implemented	Yes, multiple types of enterprise-level controls are implemented	
CTRL	**Does your organization identify management directives and organizational guidelines from which to derive control objectives, such as**	No, or control objectives are not defined	Control objectives are usually based on resilience requirements or compliance	Yes, but primarily or only from organizational-unit-level sources	Yes, from both enterprise-level and organizational-unit-level sources	

strategic objectives, resilience requirements for services, and compliance obligations?

obligations only

CTRL	**Does your organization identify and implement service-level and associated asset-level controls to protect services and assets from disruption?**	No	For a single asset type, or in very few organizational units (<10%)	For most asset types in some organizational units (10%–50%)	For most asset types in many organizational units (>50% but <100%)	Yes, for all asset types in all organizational units (100%)	
EF	**Are data for measuring key resilience indicators monitored, collected, and reported to key governance stakeholders? [EF:SG4.SP2.3]**	No	These activities are planned but have not been developed	These activities are in development	These activities have been partially implemented	Yes	Yes, and reporting is performed on a regular basis according to documented procedures
EF	**Is the success of resilience promotion activities regularly measured? [EF:SG3.SP2.2]**	No	For a few activities (<10%)	For some activities (10%–49%)	For many activities (50%–80%)	Yes, for most activities (>80%)	
EF	**Is the performance of higher level managers measured with respect to their ability to promote and communicate the importance of resilience programs and activities? [EF:SG3.SP2.3]**	No	For up to 30% of managers	For up to 70% of managers	Yes		
EF	**Are rewards and recognition programs established to support resilience acculturation? [EF.SG3.SP2.4]**	No	Yes, one or two	Yes			
EF	**Are policy statements established and disseminated that reflect higher level managers' commitments to managing operational resilience? [EF:SG3.SP3.1]**	No	No, but those commitments are expressed through other means	Yes			
EF	**Has a governance structure been developed and implemented to provide oversight for the operational resilience management system? [EF:SG4.SP1.1]**	No	In development	In progress; less than 30% complete	In progress; less than 70% complete	Yes	

EF	**Have roles and responsibilities for governance over the operational resilience management system been developed and assigned? [EF:SG4.SP1.2]**	No	In development	In progress; less than 30% complete	In progress; less than 70% complete	Yes

EF	**Have the procedures, policies, standards, guidelines, and regulations that form the basis to govern the operational resilience management system been identified? [EF:SG4.SP1.3]**	No	In development	In progress; less than 30% complete	In progress; less than 70% complete	Yes
EF	**Has a governance dashboard or scorecard been established for measuring and managing the performance of the organization's operational resilience management system? [EF:SG4.SP2.2]**	No	In development	In progress; less than 30% complete	In progress; less than 70% complete	Yes
EF	**Has a plan been developed for visible promotion of a resilience-aware culture? [EF:SG3.SP2.1]**	No	Yes	Yes, and it includes success metrics		
EF	**Do key governance stakeholders regularly review audit reports of the operational resilience management system to identify problems? [EF:SG4.SP2.4]**	No	Very few key stakeholders (<10%)	Some key stakeholders (10%- 49%)	Many key stakeholders (50%-99%)	Yes (100%)
EF	**Does a process exist for handling exceptions to acceptable behaviors (violations of resilience procedures, policies, standards, guidelines, and regulations)? [EF:SG4.SP2.5]**	No	A process is planned but has not been developed	A process is in development	A process has been partially implemented	Yes
EF	**Are key resilience indicators that do not meet established criteria identified and analyzed? [EF:SG4.SP3.1]**	No, or there are no metrics	This activity is planned but has not been developed	This activity is in development	This activity has been partially implemented	Yes
EF	**Are corrective actions developed to address performance issues when key resilience indicators do not meet established criteria? [EF:SG4.SP3.2]**	No	For very few of such cases (<10%)	For some of such cases (10%–49%)	For many of such cases (50%–80%)	Yes, for most of such cases (>80%)
EF	**Are the persons or groups that are**	Corrective actions	No	Only in an ad hoc	Yes	Yes, and they have

responsible for implementing and managing corrective actions for performance issues identified? [EF:SG4.SP3.3	are not developed	manner	the requisite skills and training

EF	**Is oversight over the operational resilience management program provided? [EF:SG2.SP2.4]**	There is no program	No	For up to 30% of strategic objectives	For up to 70% of resilience activities	Yes	Yes, and corrective actions are implemented when necessary
EF	**Have key governance stakeholders for the operational resilience management system been identified? [EF:SG4.SP2.1]**	No	In development	In progress; less than 30% complete	In progress; less than 70% complete	Yes	
EF	**Is corrective action taken as necessary to achieve critical success factors? [EF:SG1.SP2.4]**	No	For up to 30% of strategic objectives	For up to 70% of resilience activities	Yes		
EF	**Is funding for the operational resilience management program included as a regular part of the organization's strategic planning and budgeting exercise? [EF:SG3.SP1.2]**	No	For a few activities (<10%)	For some activities (10%–49%)	For many activities (50%–80%)	Yes, for most activities (>80%)	
EF	**Is an allocation of funding for the operational resilience management program approved by higher level management? [EF:SG3.SP1.3]**	No	For a few activities (<10%)	For some activities (10%–49%)	For many activities (50%–80%)	Yes, for most activities (>80%)	
EF	**Are strategic objectives (in the form of a strategic plan) used as the basis for resilience activities? [EF:SG1.SP1.2]**	Strategic objectives are not developed	No	For up to 30% of resilience activities	For up to 70% of resilience activities	Yes	
EF	**Have critical success factors been developed that reflect strategic objectives? [EF:SG1.SP2.1]**	No	Not formally, but they are generally known	Yes			
EF	**Are key performance indicators identified to measure accomplishment of each critical success factor? [EF:SG1.SP2.3]**	No	For up to 30% of strategic objectives	For up to 70% of resilience activities	Yes		
EF	**Have the services that are performed to achieve the organization's mission**	No	Only in an ad hoc manner, so probably	Yes			

been identified? [EF:SG1.SP3.1]	not all have been identified

EF	**Are the attributes of services (such as their inputs and outputs, associated assets, owners, and stakeholders) defined in service profiles? [EF:SG1.SP3.2]**	No	For up to 30% of strategic objectives	For up to 70% of resilience activities	Yes, but only two or three attributes are described for each service	Yes	Yes, and profiles are revised as needed to keep them up-to-date
EF	**Is affinity analysis or some other method used to compare organizational services against objective measures (such as strategic objectives and critical success factors) to identify high-value services? [EF:SG1.SP3.3]**	No	No, but high-value services are identified in some other way	For selected services, but high-value services are identified from that set	Yes		
EF	**Is a sound business case developed to ensure that tangible, measureable, and demonstrable value is provided to the organization for its investment in resilience activities? [EF:SG3.SP1.1]**	No	For a few activities (<10%)	For some activities (10%–49%)	For many activities (50%–80%)	Yes, for most activities (>80%)	
EF	**Are commitments to perform the activities of the operational resilience management plan obtained from staff? [EF:SG2.SP1.2]**	No, or there is no plan	For up to 30% of strategic objectives	For up to 70% of resilience activities	Yes	Yes, and they are confirmed on a cycle commensurate with the organization's strategic business planning process	
EF	**Has an operational resilience management program been established for implementing the activities of the operational resilience management plan? [EF:SG2.SP2.1]**	No, or there is no plan	For up to 30% of strategic objectives	For up to 70% of resilience activities	Yes		
EF	**Is the operational resilience management program adequately funded? [EF:SG2.SP2.2]**	There is no program	No	For a few activities (<10%)	For some activities (10%–49%)	For many activities (50%–80%)	Yes, for most activities (>80%)

EF	**Are staff assigned to execute the activities of the operational resilience management program? [EF:SG2.SP2.3]**	There is no program	No	For a few activities (<10%)	For some activities (10%–49%)	For many activities (50%–80%)	Yes, for most activities (>80%)

EF	**Is an operational resilience management plan developed in conjunction with the development of the organization's strategic plan? [EF:SG2.SP1.1]**	No	A plan is developed, but not in conjunction with the strategic plan	Yes	Yes, and it is revised on a cycle commensurate with the organization's strategic business planning process	
EF	**Is affinity analysis or some other method performed to document the relationship between the organization's strategic objectives and critical success factors? [EF:SG1.SP2.2]**		For up to 30% of strategic objectives	For up to 70% of resilience activities	Yes	
EF	**Are defined statements of the organization's mission, vision, values, and purpose readily available for use for resilience planning?**	No	One or two of those, but not all	Yes, but they are too general to be useful in resilience planning	Yes	
IMC	**Does your organization develop an incident response to prevent or limit the impact of incidents?**	No	Only for high-impact incidents	Yes, designated people plan necessary responses	Yes, according to preplanned procedures and/or strategies	
IMC	**Has your organization identified the most appropriate ways to communicate with relevant stakeholders with whom it must communicate regarding incidents?**	No	Relevant stakeholders haven't been identified, but incident information is sent to anyone who requests it	Relevant stakeholders have been identified but not categorized, so communication with them is not tailored	Communications are tailored for some types of stakeholders, such as higher level managers	Yes, for all types of stakeholders
IMC	**Has your organization developed and implemented an incident management communications plan?**	No	No, incident management communications are ad hoc	There is no communications plan, but incident management staff are trained in incident management related communications	Yes	Yes, and the plan is regularly improved based on incident communications experience
IMC	**Are incidents closed after relevant actions have been taken by your**	Yes	Yes, and they are marked as closed in the	Yes, according to a defined closure	Yes, and incidents that are not marked	

organization?	incident knowledgebase	procedure	as closed are tracked until they are resolved

IMC	**Do you perform post-incident review using root-cause analysis or other techniques to determine underlying causes of incidents?**	No	For some incidents (10%–49%)	For most incidents (50%–80%)	Yes, for almost all incidents (>80%)	Yes, for almost all incidents (>80%), and results are documented both in closure reports and in the incident knowledgebase
IMC	**Are lessons learned from incident management routinely used to improve protection, security, and/or continuity strategies?**	No, or lessons-learned information is not collected	Only lessons learned from high-impact incidents	Yes		
IMC	**Are incidents escalated to appropriate stakeholders for input and resolution?**	No	On an ad hoc basis	Yes, incident management staff know how and to whom to escalate incidents	Yes, according to predefined criteria and procedures	
IMC	**Have staff been assigned to all roles and responsibilities detailed in the incident management plan?**	No staff are assigned to incident response (there may or may not be an incident management plan)	There is no incident management plan, but some staff members are assigned responsibilities for responding to incidents	Incident management roles are assigned as needed to handle an incident	Yes, all staff roles and responsibilities are identified and assigned	
IMC	**Is there a link (through the incident knowledgebase or some other means) between your organization's incident management process and its problem management process?**	No, or there is no problem management process	There is no formal link between the processes, but some incident information is passed along to the problem management process	Yes	Yes, and problem reports are periodically reviewed to determine whether any action should be taken related to incident detection and analysis methods or incident response procedures	
IMC	**Are incidents analyzed and any needed information collected to determine an appropriate response?**	No	Only for some incidents	Yes, analysis and information collection is done for all incidents,	Yes, and extensive analysis is done for some types of	

and results are documented in incident analysis reports	incidents to determine underlying causes

IMC	**Does your organization declare incidents according to established criteria or thresholds?**	No	Incidents are declared in an ad hoc or inconsistent manner	Yes, authorized staff use identified criteria or thresholds to identify and declare incidents	Yes, and incident declaration criteria are updated based on experience with prior incidents	
IMC	**Does your organization assign a disposition (or status) to events and either close them or route them to the incident management team or other appropriate entity?**	No	No, but all events are routed to the incident management team	Yes, and dispositions are recorded in the incident knowledgebase	Yes, and the process includes periodic review of the incident knowledgebase to follow up on events that have not been closed or for which there is no disposition	
IMC	**Are events triaged—that is, categorized as to type and extent, correlated to other events, and prioritized as to the order in which they should be addressed or assigned?**	No	Some triage is done (prioritization or categorization)	Yes, depending on the type or potential impact of the event	Yes, through a defined procedure	Yes, through a defined procedure and using the organization's standard event categories and prioritization scheme
IMC	**Does your organization ensure that event evidence is properly collected, handled, documented, preserved, and protected as may be required by law or other obligations?**	No	For some types of events	For most types of events	Yes, for all types of events and as required by relevant rules, laws, regulations, and policies	
IMC	**Is there an incident knowledgebase or some other mechanism that enables consistent logging of event data?**	No	No, but there are informal methods for logging events	Yes, for some event data, such as date and time, description, and source	Yes, for comprehensive event data, such as event description, associated costs, and the assets, services, and organizational	

units that are affected by the event

IMC	**Does your organization use multiple internal and external methods and sources for detecting events?**	No	No, but everyone knows who to contact if an incident is suspected	Methods exist only for detecting events that affect technical infrastructure (e.g., network monitoring, application data monitoring)	Events are detected through numerous internal methods and sources (e.g., network and system monitoring, service desk issues, staff observations of malicious or suspicious activities)	Yes, events are detected through external as well as internal methods and sources (e.g., forwarded from law enforcement, vendors, or other security organizations, or viewed through various media channels)
IMC	**Does your organization have a documented plan for performing incident management?**	No	In some organizational units or lines of business	There is a documented plan, but no one formally commits to it	Yes, both a documented plan and documented commitments to the plan	
IMC	**Has your organization established a process for reporting events?**	No	Events are reported via email or phone to the service desk	Yes, there is an established process for documenting events and reporting them to the service desk, appropriate incident management staff, or other authorized entity		
KIM	**Are administrative, technical, and physical controls identified and implemented as needed to meet resilience requirements for information assets?**	No	Some controls are implemented, but they are not aligned with resilience requirements (or there are no documented requirements)	Controls are implemented for all high-priority information assets, but they are not aligned with resilience requirements (or there are no documented requirements)	Yes, in some organizational units or for certain categories or types of information assets	Yes
KIM	**Does your organization use an information asset sensitivity**	No	Only for classified assets	Yes, for all categories, but its use is not	Yes, for all categories	

categorization scheme that covers all categories of information assets (public, internal use only, confidential, secret, etc.)?	enforced or monitored

KIM	**Are resilience requirements (for confidentiality, integrity, and availability) assigned to information assets and documented in asset definitions?**	No	In some organizational units or for certain categories or types of information assets	documented in asset definitions	Yes	
KIM	**Using organizationally defined criteria, has your organization selected certain information assets for periodic risk assessment?**	No risk assessments are done on information assets	An initial risk assessment is done for new assets, but no periodic assessments are done	In some organizational units	Yes	
KIM	**As a result of periodic risk assessments of selected information assets, are risk mitigation strategies developed for risks the organization decides to mitigate, and are they validated by comparing them to existing strategies?**	No periodic risk assessments of selected information assets are done	Risk mitigation strategies are not developed	Risk mitigation strategies are developed but are not validated	Yes, they are developed and validated	Yes, they are developed, validated, and implemented, and risk mitigation strategies are monitored for effectiveness after implementation
KIM	**Does your organization have policies and procedures for encrypting information assets as appropriate or required for their asset sensitivity categorization?**	No, there are no such policies and procedures	There are no documented policies or procedures, but staff members know how and when to encrypt information	There are policies or procedures for encryption, but they are not tied to asset sensitivity categorizations	Yes	
KIM	**Do you implement access controls for information assets as needed to satisfy confidentiality- and privacy-related resilience requirements (including those imposed by laws and regulations)?**	No	Access controls are implemented for certain categories or types of information assets, but selection of access controls is not based on requirements of any kind	Access controls are implemented for information assets only as needed to satisfy confidentiality- and privacy-related resilience requirements imposed by laws and regulations	Yes, access controls are implemented as needed to satisfy all confidentiality- and privacy-related resilience requirements, including those imposed by laws and regulations	Yes, and access controls are managed on an ongoing basis to ensure continued satisfaction of requirements

KIM	**Are organizational guidelines followed for disposing of information assets in a manner appropriate to their resilience requirements and sensitivity categorizations and in accordance with any applicable rules, laws, and regulations?**	No	There are guidelines, but they are not well documented, communicated, or implemented	Guidelines are followed for disposing of assets in accordance with applicable rules, laws, and regulations, but not for other reasons	Guidelines for proper disposal of assets for all reasons have been communicated to all staff who are responsible for the resilience of information assets, but adherence to the guidelines is not enforced or monitored	Yes, and adherence to the guidelines is enforced and monitored
KIM	**Is the integrity of high-value information assets preserved by controlling their modification using access controls, monitoring and logging modification activity, and other means?**	No	Only access controls are used	Yes, multiple types of controls are used	Yes, and audits of modification logs are performed periodically and anomalies are addressed	
KIM	**Is the integrity of information assets preserved by using configuration control policies, procedures, and techniques to manage changes to assets?**	No	Baselines are established, but changes are not always managed	Yes, baselines are established and changes are managed through configuration control	Yes, and configuration control logs are reviewed and anomalies are addressed	
KIM	**Does your organization use controls to sustain and verify the validity and reliability of information assets as they are altered through the information processing cycle (used by a service)?**	No	There are controls and procedures in some services or for certain categories or types of information assets	Yes, data validation controls are used for information assets	Yes, and monitoring and auditing are done to periodically verify that changes are valid and authorized	
KIM	**Are high-value information assets backed up and retained so that they are available when needed?**	No, no backup is done	Some backup is done, but there are no guidelines about which	Assets that support high-value services are backed up but not necessarily	Yes, high-value information assets are backed up and	Yes, and the organization's backup and storage

information assets should be backed up	other high-value information assets such as intellectual property	retained	procedures and guidelines are periodically tested to ensure continued validity as operational conditions change

KIM	**Is the institutional knowledge of staff members that is vitally important to normal operations duplicated in some way (such as documentation or cross-training)?**	No, because staff members who may have institutional knowledge have not been identified for this purpose	Staff members who may have institutional knowledge have been identified, but their knowledge is not duplicated	Staff members with vital institutional knowledge are encourage to document their knowledge, but there are no policies or procedures for doing so	In some organizational units or for certain kinds of institutional knowledge	Yes	Yes, and procedures for regular identification, capture, and revision of institutional knowledge have been developed and implemented
KIM	**Has your organization prioritized its information assets by their importance in supporting the delivery of high-value services or some other criteria so that it knows which assets should be the focus of operational risk and resilience activities?**	No	Not formally, but that priority is generally known	In some organizational units or for certain categories or types of information assets	Yes	Yes, and the prioritization is periodically updated and validated	
MON	**Have plans for the involvement of relevant internal and external stakeholders in the monitoring process been developed?**	No	Stakeholders are involved in the monitoring process, but there is no process for identifying relevant stakeholders and no plans are developed to describe their involvement	For some (10%-49%) operational resilience management processes and activities	For many (50%-80%) operational resilience management processes and activities	Yes, for most (>80%) operational resilience management processes and activities	
MON	**Has your organization established distribution infrastructure, methods, and channels that make monitoring data available to stakeholders in the form and at the frequency they have requested?**	No, or stakeholder requirements are not identified	For some types (10%-49%) of monitoring data	For many types (50%-80%) of monitoring data	Yes, for most types (>80%) of monitoring data		
MON	**Is monitoring data relevant to the operational resilience management system collected and recorded on appropriate media according to stakeholders' requirements?**	No	Some monitoring data is collected and recorded, but stakeholder requirements are not	For some (10%-49%) operational resilience management processes and activities	For many (50%-80%) operational resilience management processes and	Yes, for most (>80%) operational resilience management processes and	

			identified		activities	activities
MON	**Have standards and parameters for collecting, handling, and storing monitoring data been developed?**	No	For some types (10%-49%) of monitoring data	For many types (50%-80%) of monitoring data	Yes, for most types (>80%) of monitoring data	

MON	**Is infrastructure in place that is sufficient for meeting monitoring requirements and program objectives?**	No, or that information is not known	Most (>80%) of the monitoring requirements specify infrastructure that is not in place	Many (50%-80%) of the monitoring requirements specify infrastructure that is not in place	Some (10%-49%) of the monitoring requirements specify infrastructure that is not in place	Very few (<10%) of the monitoring requirements specify infrastructure that is not in place
MON	**Are monitoring requirements for each stakeholder identified and documented?**	No	For some (10%-49%) operational resilience management processes and activities	For many (50%-80%) operational resilience management processes and activities	Yes, for most (>80%) operational resilience management processes and activities	Yes, for most (>80%) operational resilience management processes and activities, and the requirements are reviewed, validated, and updated on a regular basis
MON	**Have a plan and program for identifying, recording, collecting, and distributing operational resilience monitoring information been established?**	No	Some monitoring of operational resilience management processes and activities is performed, but there is no plan or program for it	Yes, a plan for a monitoring program has been developed and documented	Yes, and those responsible have committed in writing to implement and support the plan	Yes, and the plan and commitments to the plan are revised as necessary as part of an established periodic review process
MON	**Are monitoring requirements analyzed to determine whether they can be satisfied (in terms of resources and infrastructure)?**	No, or requirements are not identified	For some types (10%-49%) of operational resilience management processes and activities	For many types (50%-80%) of operational resilience management processes and activities	Yes, for most types (>80%) of operational resilience management processes and activities	
RISK	**Are risks prioritized based on assigned risk valuations to determine the risks that most need attention?**	No, or risk valuations are not determined	Risks are prioritized, but prioritization is based on some criteria other than assigned risk	Risks in some categories are prioritized based on assigned risk valuations	yes	

RISK	**Is a strategy for managing operational risk that aligns with the organization's overall enterprise risk management strategy established and maintained?**	No	Risk management is performed, but there is no documented strategy for it	There is a strategy for managing operational risk, but it doesn't align with the organization's enterprise risk management strategy (or there is no enterprise-level strategy	Yes	Yes, and the operational risk management strategy is aligned with the organization's strategic objectives
RISK	**Does your organization compare risk mitigation plans to existing service continuity plans and revise or create service continuity plans as needed?**	No	For few services (<10%)	For some services (10%–50%)	For many services (>50% but <80%)	Yes, for most services (>80%) or all high-value assets
RISK	**Does your organization compare risk mitigation plans to existing strategies for protecting assets and revise or add controls in those strategies as needed?**	No	For few assets (<10%)	For some assets (10%–50%)	For many assets (>50% but <80%)	Yes, for most assets (>80%) or all high-value assets
RISK	**Does your organization periodically review identified risks to determine whether there have been changes in the risk environment that would warrant changes in their risk dispositions?**	No	Some categories of risk, or in some organizational units or lines of business	Most categories of risk, or in most organizational units or lines of business	Yes	
RISK	**Are risk mitigation plans monitored for effectiveness?**	No, or there are no risk mitigation plans	For some categories of risk, or in some organizational units or lines of business	For most categories of risk, or in most organizational units or lines of business	Yes	
RISK	**Are risk mitigation plans developed for risks that the organization decides to mitigate?**	No	Plans are developed for some categories of risk that describe what will be done, when, and by whom	Plans are developed for all categories of risk that describe what will be done, when, and by whom	Plans are developed for all categories of risk that describe what will be done, when, and by whom; the cost of the plan, with a cost-benefit analysis; and	

identification of any residual risk that will not be addressed by the plan

RISK	**Is the disposition (Risk: acceptance, avoidance, transfer, monitor, research/defer, mitigation) of each identified risk documented and approved?**	No	For some risks (<50%) or some categories of risk	For many risks (50%–80%)	Yes, for most risks (80%–100%)		
RISK	**Are identified risks evaluated and assigned qualitative or quantitative valuations using the defined risk parameters and risk measurement criteria?**	No	Very few identified risks (<10%)	Some identified risks (10%–50%)	Many identified risks (>50% but <80%)	Yes, most identified risks (>80%)	
RISK	**Do risk statements for high-value assets include information about the potential effect on the services they support if the risk is realized?**	No, or there are no risk statements	For very few identified risks (<10%)	For some identified risks (10%–50%)	For many identified risks (>50% but <80%)	Yes, for most identified risks (>80%)	
RISK	**Does your organization use various techniques and methods to identify operational risks to high-value assets?**	No	No, but risks are documented when they become known	Risk identification is done for some high-value assets (10%–50%)	Risk identification is done for many high-value assets (>50% but <80%)	Yes, for most high-value assets (>80%)	
RISK	**Are risk parameters (operational risk thresholds and impact and probability criteria) defined for each category of risk?**	No, or risks are not categorized	For very few categories (<10%) or for some specific risks	For some categories (10%–50%)	For many categories (>50% but <100%)	Yes (100%)	
RISK	**Are operational risks categorized and organized in some way that is relevant to the organization?**	No	Some categorization is done	Some sources of risk are categorized and organized in a taxonomy	Yes		
RISK	**Does your organization categorize risks according to its defined risk categories or other forms of categorization?**	No, or risk categories are not determined	Very few identified risks (<10%)	Some identified risks (10%–50%)	Many identified risks (>50% but <80%)	Yes, most identified risks (>80%)	Yes, most identified risks (>80%), and the cause-and-effect relationship between related risks is identified

RISK	**Does your organization identify and document the sources from which operational risk to its assets and services may originate?**	No	A few general sources have been identified, but no analysis is conducted to identify most or all sources	In some organizational units or lines of business or for certain asset types	Yes, possible risk sources are identified and documented

RISK	**Are criteria for measuring and evaluating the impact of realized risk defined and documented for organizational impact areas?**	No, or organizational impact areas have not been defined	Some risk measurement and evaluation criteria have been developed, but organizational impact areas have not been identified	For some organizational units or lines of business	Yes	Yes, and they are applied consistently across all operational risks
SC	**Are changes made to service continuity plans based on organizationally defined change criteria?**	No	There are no documented criteria or conditions, but service continuity plans are updated in response to various events and conditions	Yes	Yes, and versions of existing plans are incremented according to the organization's versioning protocol and standards	Yes, and new versions of plans are communicated to relevant stakeholders
SC	**Have a program, standards, and schedules for testing service continuity plans been implemented?**	No	There are schedules but no test program or standards	There are schedules and either a test program or standards	Yes	
SC	**Are service continuity test plans developed and reviewed with stakeholders before being implemented?**	No	Test plans are developed and documented for some services (<50%)	Test plans are developed and documented for many services (50%-80%)	Yes, test plans are developed and documented for most or all services (>80%) and are reviewed with stakeholders	
SC	**Are service continuity plans tested on an organizationally defined basis using necessary staff and resources, and are the results documented?**	No	Some plans (10%-49%)	Many plans (50%-80%)	Yes, most plans (>80%)	Yes, and documentation of results is done in accordance with the organization's testing standards
SC	**Are test results compared with test objectives to identify needed improvements to both service continuity plans and test plans?]**	No	Needed improvements to service continuity plans are identified and documented	Yes	Yes, needed improvements to both service continuity plans and test plans are	

identified and
documented

SC	**Do owners of service continuity plans execute specific plans in response to specific conditions?**	No	No, they execute plans only when directed to (by the incident management team, higher level managers, or others)	Yes, owners of service continuity plans know the conditions under which plans must be executed and have the authority and responsibility to execute the plans if necessary		
SC	**Have criteria for making changes to service continuity plans been defined?**	No	No, but criteria for making changes to service continuity plans are generally known by plan owners	Yes, criteria for making changes to service continuity plans have been developed and documented		
SC	**Are vital records and databases identified and documented?**	No	They are identified and documented within certain organizational units or lines of business but not organization-wide	Yes	Yes, including a directory of vital staff and their specific roles in high-value services	Yes, and controls are in place to ensure that vital records and databases are protected, accessible, and usable if a disruption occurs
SC	**Are conflicts between service continuity plans (in use of resources) identified through plan review and resolved?**	No	Conflicts aren't identified through plan review, but if they are identified through plan testing or execution, they are resolved	Yes, conflicts are identified, and most conflicts are reduced or eliminated	Yes, conflicts are reduced or eliminated, and plans are rewritten and revised as necessary	
SC	**Are post-execution reviews of service continuity plans performed to identify corrective actions?**	No	For some plans (10%-49%)	For many plans (50%-80%)	Yes, for most plans (>80%)	Yes, for most plans (>80%), and areas of improvement for plans are documented
SC	**Has your organization developed and documented a plan for its service continuity process?**	No, there is no service continuity process	No, no plan has been developed or documented for the	There is no plan, but some aspects of the service continuity	Yes, planning is performed	Yes, planning is performed and a program has been

service continuity process	process are documented	developed and documented

SC	**Does your organization provide training as needed to staff assigned to service continuity plans?**	No	The organization doesn't identify skill gaps, but training is available	yes	Yes, and training materials and resources have been developed to conduct training on a regular and ongoing basis	
SC	**Is there a service continuity plan repository or database, and are access controls used to ensure that service continuity plans can be accessed only by authorized individuals?**	No	There is a repository for service continuity plans, but no access controls are used on it	Yes, service continuity plans are stored and access controls are used		
SC	**Does your organization identify service continuity plans to be developed?**	No	Existing service continuity plans are maintained, but no means are used to identify new plans needed	Yes, a single means is used	Yes, multiple means are used, such as business impact analysis, risk assessment activities, and lessons learned from past disruptions	
SC	**Are any external entities that the organization depends on to provide high-value services, such as public utilities and contractors, identified and documented?**	No	There are records that identify and document such external entities, but specific dependencies of high-value services on those entities isn't documented	Yes		
SC	**Are the associations between the high-value services of the organization and the assets that support them (people, information, technology, and facilities) identified?**	High-value services have not been identified	High-value services have been identified but not associations between them and their supporting assets	Associations have been identified between some high-value services (<50%) and their supporting assets or for certain categories of supporting assets	Associations between many high-value services (50%-80%) and their supporting assets have been identified, but certain	Yes, for most or all high-value services (>80%) and their supporting assets

categories of supporting assets tend to be overlooked

SC	**Are service continuity guidelines and standards (regarding standard content of plans, testing requirements, plan versioning, etc.) developed and communicated?**	No	Basic guidelines and standards, such as requirements for plans and plan creation templates, have been developed for some aspects of the service continuity program, but they are not well communicated	Additional guidelines and standards, such as standard content of plans, testing requirements for plans, stakeholder involvement, and plan change control, have been developed and communicated for some aspects of the service continuity program	Yes, guidelines and standards have been developed and communicated for most aspects of the service continuity program		
SC	**Are service continuity plans objectively reviewed to ensure that they conform to the organization's standards and requirements for plan development?**	No	Plans are evaluated against development standards or guidelines but not against requirements	Plans are evaluated against requirements but not against development standards or guidelines	Yes	Yes, and appropriate plan updates and remediation actions are developed if necessary	
SC	**Are staff members assigned to execute specific service continuity plans?**	No	No, but there is a list of staff that is required to execute service continuity plans	Yes			
TM	**Are audits of technology asset modification logs performed periodically, and are any anomalies discovered addressed?**	There are no technology asset modification logs	No	Audits are rarely performed, but any anomalies discovered are addressed	Yes		
TM	**Are selected technology assets placed under configuration management using organizational standards, guidelines, policies, and tools?**	No	There are no organizational standards, etc., but some technology assets are placed under configuration control	In some organizational units or for certain categories or types of technology assets	Yes	Yes, and configuration control logs are reviewed periodically to identify anomalies	Yes, and the integrity of configuration item baselines is audited regularly to ensure that they are complete and correct
TM	**Are changes to technology assets managed using organizational change**	No	There are no organizational policies,	In some organizational units or for certain	Yes	Yes, including analysis of impacts	

control policies, procedures and techniques?	etc., but change management is done for some technology assets	categories or types of technology assets	of changes proposed and required approval of changes by relevant stakeholders

TM	**Does your organization use release management or iteration control for technology assets that are released into the production environment?**	No	Only for some types of technology assets	For most types of technology assets	Yes	
TM	**Does your organization help ensure the availability and functionality of high-value technology assets by developing plans to sustain them (such as business continuity plans)?**	No	Only for a few types of high-value technology assets	Yes	Yes, and the plans refer to metrics such as availability metrics, recovery time objectives, and recovery time objectives	
TM	**Are corrective, preventive, and other types of maintenance performed on technology assets that require it?**	No	Corrective maintenance is performed when there is a maintenance issue	Yes, all types of maintenance are performed	Yes, all types of maintenance are performed, and equipment suppliers' recommended service intervals and specifications are used when available	
TM	**Does your organization have a strategy for managing the interoperability of technology assets?**	No	No, but some interoperability architecture and design principles are commonly used	Interoperability standards have been established related to architecture and design, minimizing complexity, preventing operational risk, etc.	Yes, there is a strategy for managing interoperability that is used across the enterprise	Yes, and risks that are identified through interoperability management are referred to the risk management process
TM	**Does your organization implement access management policies and procedures for requesting and approving access privileges to technology assets?**	No	For few technology assets (<10%)	For some technology assets (10%–49%)	For many technology assets (50%–80%)	Yes, for most technology assets (>80%)
TM	**Is the effectiveness of controls monitored so as to identify any**	No	For certain categories of controls or for certain	For most controls	Yes, for all controls	

deficiencies?

categories or types of technology assets

TM	**Is capacity management and planning done for technology assets that require it?**	No	Yes, for a few technology assets (<10%)	Yes, for some technology assets (10%–49%)	Yes, for many technology assets (50%–80%)	Yes, for most technology assets (>80%)	Yes, for most technology assets (>80%), and capacity management strategies are periodically validated and updated based on operational and organizational environmental changes
TM	**Does your organization prioritize Technology assets relative to their importance in supporting the delivery of high-value services?**	No	Few technology assets (<10%)	Some technology assets (10%–49%)	Many technology assets (50%–80%)	Yes, most technology assets (>80%)	
TM	**As a result of periodic risk assessments of selected technology assets, are risk mitigation strategies developed and implemented for risks the organization decides to mitigate?**	No periodic risk assessments of technology assets are done	Risk mitigation strategies are not developed	Yes, they are developed and implemented	Yes, they are developed and implemented, and risk mitigation strategies are monitored for effectiveness after implementation		
TM	**Using organizationally defined criteria, does your organization periodically identify and assess risks to technology assets?**	No risk assessments are done on technology assets	An initial risk assessment is done for new assets, but no periodic assessments are done	For some categories or types of technology assets	Yes		
TM	**Are controls over the design, construction, and acquisition of technology assets specified?**	No	In very few organizational units or for one or two categories or types of technology assets	In some organizational units or for some categories or types of technology assets	Yes		
TM	**Are administrative, technical, and physical controls identified and**	No	Some controls are implemented, but they	Controls are implemented for all	In some organizational units	Yes	

implemented as needed to meet resilience requirements for technology assets?	are not aligned with resilience requirements (or there are no documented requirements)	high-priority technology assets, but they are not aligned with resilience requirements (or there are no documented requirements)	or for certain categories or types of technology assets

TM	**Are resilience requirements that have been defined assigned to technology assets?**	No	In some organizational units or for certain categories or types of technology assets	Resilience requirements are assigned and are documented in some manner, but they are not documented in asset definitions	Yes	
TM	**Are technology assets that specifically support execution of service continuity and service restoration plans identified and documented?**	No	For a few service continuity plans (<10%)	For some service continuity plans (10%–49	For many service continuity plans (50%–80%)	Yes, for most (>80%) service continuity plans
TM	**Have organizationally acceptable tools, techniques, and methods for controlling access to technology assets been established?**	No	For few technology assets (<10%)	For some technology assets (10%–49%)	For many technology assets (50%–80%)	Yes, for most technology assets (>80%)
TM	**Does your organization identify staff authorized to modify technology assets and ensure that their access privileges align with their current job responsibilities?**	No	Such staff are identified, but they tend to just be given extensive privileges	Such staff are identified, and their privileges are scrutinized if they change jobs	Such staff are identified, and their privileges are scrutinized if there is any change at all in their job responsibilities	
VAR	**Does your organization develop resolution strategies for vulnerabilities to which exposure must be reduced or eliminated (if they require more than a simple fix such as a patch supplied by a software vendor)?**	No	No, vulnerability management staff handle resolution activities	Yes, workarounds for identified vulnerabilities are developed and implemented	Yes, and relevant stakeholders are informed of resolution activities	
VAR	**Are vulnerabilities analyzed to determine whether they have to be reduced or eliminated, and are they prioritized for disposition?**	No	No analysis is done, but certain kinds of vulnerabilities are routinely fixed through methods such as patch management	Yes	Yes, and documented prioritization guidelines are used to sort and prioritize vulnerabilities consistently	

according to their relevance to the organization

VAR	**Does your organization have a process for actively discovering vulnerabilities?**	No	Vulnerability discovery is done by performing internal vulnerability assessments and by subscribing to vulnerability catalogs and vendor notification lists	Vulnerabilities are discovered as part of a periodic threat and risk assessment or audit process	Yes, there is a process for extensive vulnerability discovery, using multiple sources and tools and a vulnerability repository, and staff receive training as needed		
VAR	**Are reputable sources of vulnerability information, both internal and external, identified in your organization?**	No	A few sources of vulnerability information have been indentified and are used	Yes, multiple sources of vulnerability information have been identified and are used	Yes, multiple sources, and the source list is updated as new sources become available		
VAR	**Has your organization developed an operational vulnerability analysis and resolution strategy?**	No	No strategy has been developed, but some vulnerability analysis and resolution activities are being performed	There is no strategy, but resources are assigned to vulnerability analysis and resolution roles and responsibilities	Yes	Yes, and the strategy is communicated to all relevant stakeholders	Yes, and stakeholders' commitment to the activities described in the strategy has been obtained
VAR	**Is root-cause analysis performed on identified vulnerabilities using appropriate tools, techniques and methods?**	No	Yes, on some vulnerabilities	Yes, on most vulnerabilities that warrant it	Yes, on most vulnerabilities that warrant it, and strategies to address root causes are developed, implemented, and monitored		
VAR	**Does your organization define the scope of its vulnerability analysis and resolution activities by identifying the high-value assets and related operational environments that must be**	No	Yes, but for information and technology assets only	Yes, for all asset types (information, technology, and facilities)	Yes, for all asset types , and the scope of vulnerability analysis and resolution activities is documented		

examined for vulnerabilities?

160