Carnegie Mellon University
Software Engineering Institute

A Targeted Improvement Plan for Service Continuity

Andrew Hoover
Gavin Jurecko
Jeffrey Pinckard
Phillip Scolieri
Robert Vrtis

April 2019

TECHNICAL NOTE
CMU/SEI-2019-TN-002

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM19-0113

Table of Contents

List of Tables

Abstract

This technical note describes how an organization can leverage the results of a Cyber Resilience Review to create a Targeted Improvement Plan for its service continuity management (SCM). An organization can use the Cyber Resilience Review (CRR) results and prioritize SCM-specific and supporting practices using a SCM improvement profile to develop a long-term plan. The suggested Targeted Improvement Plan (TIP) approach engages the organization's business continuity professionals, information technology operations management staff, and security management team (physical and cyber) to create a resilient organization. (In some organizations, it will be appropriate to engage the operational technology team as well.) The technical note includes a SCM Improvement Template that prioritizes all the CRR practices; it places a higher priority on those practices that enable service continuity. It describes how an organization can integrate the results of a recent CRR to create a prioritized list of practices the organization should consider implementing. This list informs decisions that take into account the organization's unique risk environment to develop a plan. This approach to developing and implementing a SCM program supports organization-specific, mission-focused objectives to protect and sustain a critical, cyber-dependent service during times of stress.

1 Introduction

Service continuity management (SCM) is a business issue that transcends technology and must be defined as a collection of policies, standards, processes, and tools through which organizations maintain their ability to accomplish their mission when significant impact to a critical service has occurred.

Effective SCM requires a strategy that is agreed upon at the most senior levels of the organization (at the board level if a board exists) and fully endorsed by the CEO. The strategy should define the direction and identify the resources and high-level methods that are necessary to meet specific service-level objectives. This enabling step is critical to the development of a Service Continuity Management program and should be undertaken at the start of a plan development process.

The Cyber Resilience Review (CRR) allows organizations to examine the cyber resilience of a specific service that is critical to the accomplishment of their organization's mission. Cyber resilience is the ability of the organization to protect and sustain this critical, cyber-dependent service during times of stress. SCM supports the cyber resilience of this critical service.

In some organizations a SCM program may exist, but may not integrate the cyber aspects necessary in today's business environment. Many small and mid-sized organizations may have only undertaken this effort recently. Implementing a SCM program takes time and resources. A plan that takes into consideration the logical and efficient use of available resources and an organization's risk tolerance must be developed. Risk tolerance is defined by an organization's senior management and reflects the impact senior management is willing to tolerate based on the likelihood that impact will occur. Implementing a SCM program will reflect an organization's risk tolerance in how the organization will allocate available resources and the priority placed on implementing the recommended practices. An organization may choose not to implement recommended practices based on its analysis of the risk that results from this decision.

This document acts as a guide to help an organization develop a SCM Targeted Improvement Plan (TIP) using the SCM Improvement Template found in the appendix. Organizations that have completed a CRR and seek to improve their cyber resilience by focusing on improving their SCM Program will find this guide very helpful.

2 Intended Audience

The intended audience for this guide is a small to mid-sized organization that has already participated in a CRR (either a self-assessment or a facilitated assessment), although organizations that have not participated in a CRR will also find the guide useful. Small to mid-sized organizations often have limited personnel and resources. This guide is intended to aid in focusing these resources on developing a robust SCM program and assumes that the organization has the support of senior management for its efforts. While focused on small and mid-sized organizations, the guide contains information that is extremely useful for organizations of all sizes and levels of maturity.

The audience includes executives who establish policies and priorities for incident management, managers and planners who convert executive decisions into plans, and those individuals in the organization who manage or mitigate cybersecurity risks. It also includes the operations staff who implement the service continuity plans and participate in the response to cyber and physical disruptions.

While each organization is different, common participants and roles they play are shown in the table below. (Note that organizational element titles are generic and may not match all organizations.)

Table 1: Organizational Element and Role in Planning

Organizational Element	Contribution to SC Plan
Senior Management (C-suite)	Mission, vision, priorities
Senior Management (C-suite)	Executive mandate to implement SC
Senior Management (C-suite)	Risk appetite/tolerance
Senior Management (C-suite)	Funding
Line Of Business and C-suite	Mandate and commitment to test plan
Legal	Identify compliance mandates
Legal and Contracts	Parameters for managing external dependencies
Risk Manager	Risk assessment and defined risks to mitigate
Line Of Business and Risk Manager	Execution “trigger” (disruption tolerance)
Line Of Business and Risk Manager	Desired “maturity” in chosen practice model
Line Of Business and Human Resources	Staffing
Line Of Business and Human Resources	Training management and awareness
Line Of Business	Desired SC practice model to follow
Line Of Business	Desired state (RTO/RPO)
Line Of Business	Write and update plans
Line Of Business	Additions/mergers/acquisitions integration into the line of business
Line Of Business	Exercise and test plan

Organizational Element	Contribution to SC Plan
Line Of Business	Improve plan and adjust strategy
Line Of Business	Change management process
Network Operations	Capacity management
Network Operations	Detect and analyze input to incident management
Network Operations and Risk Manager	Situational awareness/new threats
Incident Management	Incident declaration based on pre-determined criteria

3 Purpose of this Guide

This guide is intended for use by organizations interested in taking action based on their CRR results by developing a plan for creating or improving a SCM program (completion of a CRR is not required to make use of this guide). The domain-specific template in this guide recommends a priority for every CRR practice, highlighting those that most directly support the development of a SCM Improvement plan. The prioritization provided by the template informs the risk-based decision-making process on improvement plans to enhance performance and meet organizational requirements for mission assurance. Applying practices from all domains to improve an organization's SCM capability improves that organization's overall cybersecurity and operational resilience. Using the template to support the objective of improving service continuity emphasizes the need to implement practices from other CRR domains. For example, identifying and prioritizing external dependencies from the External Dependencies domain and establishing technology baselines from the Configuration and Change Management domain all help in planning for SCM.

4 Developing a Targeted Improvement Plan

When developing a targeted improvement plan, the question of "What do I do first?" must be addressed. The CRR lists 167 maturity indicator level 1 practices that an organization should use in designing and implementing a cyber resilience program. In an effort to identify which of these practices are the most important to the implementation of a SCM program, the team developed the SCM Improvement Template provided in the appendix. This template ranks each of the 167 practices based on the premise that with limited resources, choices must be made. The template ranks each practice into one of four stages. Each stage is defined follows:

> Stage 1 – Essential to implementing a base SCM program but implementing only Stage 1 practices is not considered sufficient for a complete program.
>
> Stage 2 – Additional practices required for completing the implementation of a SCM program. Stage 1 and 2 practices are considered the minimum for a complete implementation.
>
> Stage 3 – Practices that directly support the integration of the SCM program with the organization's cybersecurity management program.
>
> Stage 4 – Practices that support the implementation of an organization's cybersecurity management program.

The template can be used to create a prioritized list that informs decisions that account for the organization's unique risk environment to develop a plan. The specific sequence and priority an organization assigns to each of the practices will be based on that organization's mission, resources, and risk tolerance. Having participated in a CRR, an organization has a baseline assessment of how it is currently implementing each of the 167 cyber resilience practices. The organization can use the results of the CRR and the recommended stages of the improvement template to inform decisions it must make to create a Targeted Improvement Plan. This approach to developing and implementing a SCM program supports organization-specific, mission-focused objectives to protect and sustain a critical, cyber-dependent service during times of stress.

Appendix Using the SCM Improvement Template

How to Use the Template

In working with the SCM Improvement Template, you'll note it is ordered by domain to match the CRR assessment report. The column labeled Implementation Stage indicates the stage associated with that practice (Stage 1, 2, 3, 4) as recommended by this guide.

Table 2: Design of the SCM Improvement Template

	Service Continuity Management Practice Implementation Stages		Implementation Stage	CRR Response	Gap Stage	Priority
1 Asset Management						
The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services.						
	Goal 1 – Services are identified and prioritized.					
	1.	Are services identified? [SC:SG2.SP1]	1	Yes	C	
	2.	Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	1	No	1	
	3.	Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified, and communicated? [EF:SG1.SP1]	3	Inc	3	
	4.	Are the organization's mission, objectives, and activities prioritized? [EF:SG1.SP3]	1	Inc	1	

Using the three additional columns (CRR Response, Gap Stage, and Priority) your organization can begin to develop its Targeted Improvement Plan by following the steps below.

Record the organization's current baseline based on the CRR in the second column (CRR Response). In the third column (Gap Stage), record a C (complete) if the CRR Response is Yes; if the CRR Response is No or Incomplete, this indicates there is a gap. Record the number of the Implementation Stage from column one. The fourth column will be decided based on your organization's risk tolerance and available resources.

When creating the TIP, remember that Stage 1 and 2 practices are considered required for implementing a SCM program. Practices that are fully implemented (indicated by a Yes response during the CRR) are not typically considered as candidates for improvement. A complete (C) in column 3 indicates a practice that is already fully implemented. Practices that have a 1 or 2 in column 3 (Gap Stage) fall below the recommended implementation state; these are gaps and would warrant consideration for immediate improvement. If resources do not allow taking on all gaps at once, Phase 1 practices should be considered a top priority. Consider the implementation stages indicated in the template as a recommended path for improvement. Your organization can change the recommended implementation stage, making it lower or higher, based on its own risk analysis.

In this manner, your organization can develop a roadmap providing the recommended prioritization found by completing the template, informed by the results of the CRR, using the Targeted Improvement Plan.

Template

The pages following present the SCM Improvement Template for use in developing a Targeted Improvement Plan.

Table 3: Service Continuity Management Improvement Template

	Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
1 Asset Management					
The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services.					
	Goal 1 – Services are identified and prioritized.				
1.	Are services identified? [SC:SG2.SP1]	1			
2.	Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	1			
3.	Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified, and communicated? [EF:SG1.SP1]	3			
4.	Are the organization's mission, objectives, and activities prioritized? [EF:SG1.SP3]	1			
	Goal 2 – Assets are inventoried, and authority and responsibility for these assets is established.				
1.	Are the assets that directly support the critical service inventoried (technology includes hardware, software, and external information systems)? [ADM:SG1.SP1]				
	People	1			
	Information	1			
	Technology	1			
	Facilities	1			
2.	Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]				
	People	1			
	Information	1			
	Technology	1			
	Facilities	1			
3.	Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]				
	People	2			
	Information	1			
	Technology	1			
	Facilities	1			

		Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
	4.	Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]				
		People	2			
		Information	1			
		Technology	1			
		Facilities	1			
	5.	Are organizational communications and data flows mapped and documented in the asset inventory? [ADM:SG1.SP2]	2			
	Goal 3 – The relationship between assets and the services they support is established.					
	1.	Are the associations between assets and the critical service they support documented? [ADM:SG2.SP1]				
		People	2			
		Information	1			
		Technology	1			
		Facilities	1			
	2.	Are confidentiality, integrity, and availability requirements established for each service-related asset? [RRD:SG2.SP1]				
		People	2			
		Information	1			
		Technology	1			
		Facilities	1			
	Goal 4 – The asset inventory is managed.					
	1.	Have change criteria been established for asset descriptions? [ADM:SG3.SP1]				
		People	3			
		Information	3			
		Technology	3			
		Facilities	3			

		Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
	2.	Are asset descriptions updated when changes to assets occur? [ADM:SG3.SP2]				
		People	2			
		Information	2			
		Technology	2			
		Facilities	2			
	Goal 5 – Access to assets is managed.					
	1.	Is access (including identities and credentials) to assets granted based on their protection requirements? [AM:SG1.SP1]				
		Information	1			
		Technology	1			
		Facilities	1			
	2.	Are access (including identities and credentials) requests reviewed and approved by the asset owner? [AM:SG1.SP1]				
		Information	2			
		Technology	2			
		Facilities	2			
	3.	Are access privileges reviewed to identify excessive or inappropriate privileges? [AM:SG1.SP3]				
		Information	3			
		Technology	3			
		Facilities	3			
	4.	Are access privileges modified as a result of reviews? [AM:SG1.SP3]				
		Information	3			
		Technology	3			
		Facilities	3			
	5.	Are access permissions managed incorporating the principle of least privilege? [AM:SG1.SP1]				
		Information	3			
		Technology	3			
		Facilities	3			

Service Continuity Management Practice Implementation Stages			Implementation Stage	CRR Response	Gap Stage	Priority
	6.	Are access permissions managed incorporating the principle of separation of duties? [AM:SG1.SP1]				
		Information	3			
		Technology	3			
		Facilities	3			
	Goal 6 – Information assets are categorized and managed to ensure the sustainment and protection of the critical service.					
	1.	Are information assets categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, secret)? [KIM:SG1.SP2]	3			
	2.	Is the categorization of information assets monitored and enforced? [KIM:SG1.SP2]	4			
	3.	Are there policies and procedures for the proper labeling and handling of information assets? [KIM:SG1.SP2]	4			
	4.	Are all staff members who handle information assets (including those who are external to the organization, such as contractors) trained in the use of information categories? [KIM:SG1.SP2]	4			
	5.	Are high-value information assets backed up and retained? [KIM:SG6.SP1]	1			
	6.	Do guidelines exist for properly disposing of information assets? [KIM:SG4.SP3]	4			
	7.	Is adherence to information asset disposal guidelines monitored and enforced? [KIM:SG4.SP3]	4			
	Goal 7 – Facility assets supporting the critical service are prioritized and managed.					
	1.	Are facilities prioritized based on potential impact to the critical service, to identify those that should be the focus of protection and sustainment activities? [EC:SG1.SP1]	1			
	2.	Is the prioritization of facilities reviewed and validated? [EC:SG1.SP1]	3			
	3.	Are protection and sustainment requirements of the critical service considered during the selection of facilities? [EC:SG2.SP2]	1			
2 Controls Management						
The purpose of Controls Management is to identify, analyze, and manage controls in a critical service's operating environment.						
	Goal 1 – Control objectives are established.					
	1.	Have control objectives been established for assets (technology, information, facilities, and people) required for delivery of the critical service? [CTRL:SG1.SP1]				
		People	*2*			

		Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
		Information	*2*			
		Technology	*2*			
		Facilities	*2*			
	2.	Are control objectives prioritized according to their potential to affect the critical service? [CTRL:SG1.SP1]	*2*			
	Goal 2 – Controls are implemented.					
	1.	Have controls been implemented to achieve the control objectives established for the critical service? [CTRL:SG2.SP1]	*2*			
	2.	Have controls been implemented, incorporating network segregation where appropriate, to protect network integrity? [CTRL:SG2.SP1]	3			
	3.	Have controls been implemented to protect data-at-rest? [CTRL:SG2.SP1], [KIM:SG4.SP2]	3			
	4.	Have controls been implemented to protect data-in-transit? [CTRL:SG2.SP1], [KIM:SG4.SP1], [KIM:SG4.SP2]	3			
	5.	Have controls been implemented to protect against data leaks? [CTRL:SG2.SP1], [KIM:SG4.SP1], [KIM:SG4.SP2]	3			
	6.	Have audit/log records been determined, documented, implemented, and reviewed in accordance with policy? [CTRL:SG2.SP1], [MON:SG1.SP3]	3			
	7.	Have controls been implemented to protect and restrict the use of removable media in accordance with policy? [CTRL:SG2.SP1], [TM:SG2.SP2]	3			
	8.	Have controls been implemented to protect communication and control networks? [CTRL:SG2.SP1], [TM:SG2.SP2]	3			
	9.	Have cybersecurity human resource practices been implemented for the critical service (e.g., de-provisioning, personnel screening)? [CTRL:SG2.SP1], [HRM:SG3.SP1]	3			
	10.	Is access to systems and assets controlled by incorporating the principle of least functionality (e.g., whitelisting, blacklisting, etc.)? [CTRL:SG2.SP1], [TM:SG2.SP2]	3			
	Goal 3 – Control designs are analyzed to ensure they satisfy control objectives.					
	1.	Are control designs analyzed to identify gaps where control objectives are not adequately satisfied? [CTRL:SG3.SP1]				
		People	3			
		Information	3			
		Technology	3			
		Facilities	3			
	2.	As a result of the controls analysis, are new controls introduced or existing controls modified to address gaps? [CTRL:SG3.SP1]	3			

	Service Continuity Management Practice Implementation Stages		Implementation Stage	CRR Response	Gap Stage	Priority
	Goal 4 – The internal control system assessed to ensure control objectives are met.					
	1.	Is the performance of controls assessed on a scheduled basis to verify they continue to meet control objectives? [CTRL:SG4.SP1]				
		People	3			
		Information	3			
		Technology	3			
		Facilities	3			
	2.	As a result of scheduled assessments, are new controls introduced or existing controls modified to address problem areas? [CTRL:SG4.SP1]	3			
3 Configuration and Change Management						
The purpose of Configuration and Change Management is to establish processes to ensure the integrity of assets using change control and change control audits.						
	Goal 1 – The life cycle of assets is managed.					
	1.	Is a change management process used to manage modifications to assets? [ADM:SG3.SP2]				
		Information	1			
		Technology	1			
		Facilities	1			
	2.	Are resilience requirements evaluated as a result of changes to assets? [RRM:SG1.SP3]				
		Information	2			
		Technology	2			
		Facilities	2			
	3.	Is capacity management and planning performed for assets? [TM:SG5.SP3]	3			
	4.	Are change requests tracked to closure? [TM:SG4.SP3]	3			
	5.	Are stakeholders notified when they are affected by changes to assets? [ADM:SG3.SP2]	2			
	6.	Is a System Development Life Cycle implemented to manage systems supporting the critical service? [ADM:SG3.SP2], [RTSE:SG2.SP2]	4			
	Goal 2 – The integrity of technology and information assets is managed.					
	1.	Is configuration management performed for technology assets? [TM:SG4.SP2]	2			
	2.	Are techniques in use to detect changes to technology assets? [TM:SG4.SP3]	3			
	3.	Are modifications to technology assets reviewed? [TM:SG4.SP2; TM:SG4.SP.3]	3			
	4.	Are integrity requirements used to determine which staff members are authorized to modify information assets? [KIM:SG5.SP1]	3			

		Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
	5.	Is the integrity of information assets monitored? [KIM:SG5SP3]	3			
	6.	Are unauthorized or unexplained modifications to technology assets addressed? [TM:SG4.SP2; TM:SG4.SP3]	3			
	7.	Are modifications to technology assets tested before being committed to production systems? [TM:SG4.SP4]	3			
	8.	Has a process for managing access to technology assets been implemented? [TM:SG4.SP1]	3			
	9.	Is the maintenance and repair of assets performed and logged in a timely manner? [ADM:SG3.SP2], [TM:SG5.SP2]	4			
	10.	Is the maintenance and repair of assets performed with approved and controlled tools and/or methods? [ADM:SG3.SP2], [TM:SG5.SP2]	4			
	11.	Is the remote maintenance and repair of assets approved, logged, and performed in a manner that prevents unauthorized access? [ADM:SG3.SP2], [TM:SG5.SP2]	4			
	Goal 3 – Asset configuration baselines are established.					
	1.	Do technology assets have configuration baselines? [TM:SG4.SP2]	2			
	2.	Is approval obtained for proposed changes to baselines? [TM:SG4.SP3]	3			
	3.	Has a baseline of network operations been established? [TM:SG4.SP2]	4			
	4.	Is the baseline of network operations managed? [TM:SG4.SP2]	4			
	5.	Has a baseline of expected data flows for users and systems been established? [TM:SG4.SP2]	4			
	6.	Is the baseline of expected data flows for users and systems managed? [TM:SG4.SP2]	4			
4 Vulnerability Management						
The purpose of Vulnerability Management is to identify, analyze, and manage vulnerabilities in a critical service's operating environment.						
	Goal 1 – Preparation for vulnerability analysis and resolution activities is conducted.					
	1.	Has a vulnerability analysis and resolution strategy been developed? [VAR: SG1.SP2]				
		People	3			
		Information	3			
		Technology	3			
		Facilities	3			
	2.	Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets? [VAR: SG1.SP2]				
		People	4			
		Information	3			

		Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
		Technology	3			
		Facilities	3			
	3.	Is there a standard set of tools and/or methods in use to detect malicious code in assets? [VAR:SG1.SP2]	3			
	4.	Is there a standard set of tools and/or methods in use to detect unauthorized mobile code in assets? [VAR:SG1.SP2]	3			
	5.	Is there a standard set of tools and/or methods in use to monitor assets for unauthorized personnel, connections, devices, and software? [VAR:SG1.SP2]	3			
	Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.					
	1.	Have sources of vulnerability information been identified? [VAR: SG2.SP1]				
		Information	4			
		Technology	4			
		Facilities	4			
	2.	Is the information from these sources kept current? [VAR: SG2.SP1]				
		Information	4			
		Technology	4			
		Facilities	4			
	3.	Are vulnerabilities being actively discovered? [VAR: SG2.SP2]				
		Information	4			
		Technology	4			
		Facilities	4			
	4.	Are vulnerabilities categorized and prioritized? [VAR: SG2.SP3]				
		Information	4			
		Technology	4			
		Facilities	4			
	5.	Are vulnerabilities analyzed to determine relevance to the organization? [VAR: SG2.SP3]				
		Information	4			
		Technology	4			
		Facilities	4			
	6.	Is a repository used for recording information about vulnerabilities and their resolution? [VAR: SG2.SP2]				
		Information	4			
		Technology	4			
		Facilities	4			
	Goal 3 – Exposure to identified vulnerabilities is managed.					
	1.	Are actions taken to manage exposure to identified vulnerabilities? [VAR: SG3.SP1]	2			

		Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
	2.	Is the effectiveness of vulnerability mitigation reviewed? [VAR:SG3.SP1]	4			
	3.	Is the status of unresolved vulnerabilities monitored? [VAR: SG3.SP1]	4			
	Goal 4 – The root causes of vulnerabilities are addressed.					
	1.	Are underlying causes for vulnerabilities identified (through root-cause analysis or other means) and addressed? [VAR: SG4.SP1]	3			
5 Incident Management						
The purpose of Incident Management is to establish processes to identify and analyze events, detect incidents, and determine an organizational response.						
	Goal 1 – A process for identifying, analyzing, responding to, and learning from incidents established.					
	1.	Does the organization have a plan for managing incidents? [IMC:SG1.SP1]	1			
	2.	Is the incident management plan reviewed and updated? [IMC:SG1.SP1]	3			
	3.	Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2]	3			
	4.	Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2]	2			
	Goal 2 – A process for detecting, reporting, triaging, and analyzing events established.					
	1.	Are events detected and reported (to include cybersecurity events related to personnel activity, network activity, the physical environment, and information)? [IMC:SG2.SP1]	2			
	2.	Is event data logged in an incident knowledgebase or similar mechanism? [IMC:SG2.SP2]	3			
	3.	Are events categorized? [IMC:SG2.SP4]	3			
	4.	Are events analyzed to determine if they are related to other events? [IMC:SG2.SP4]	3			
	5.	Are events prioritized? [IMC:SG2.SP4]	3			
	6.	Is the status of events tracked? [IMC:SG2.SP4]	3			
	7.	Are events tracked to resolution? [IMC:SG2.SP4]	3			
	8.	Have requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes been identified? [IMC:SG2.SP3]	4			
	9.	Is there a process to ensure event evidence is handled as required by law or other obligations? [IMC:SG2.SP3]	4			
	Goal 3 – Incidents are declared and analyzed.					
	1.	Are incidents declared? [IMC:SG3.SP1]	2			
	2.	Have criteria for the declaration of an incident been established? [IMC.SG3.SP1]	2			
	3.	Are incidents analyzed to determine a response? [IMC:SG3.SP2]	2			

	Service Continuity Management Practice Implementation Stages		Implementation Stage	CRR Response	Gap Stage	Priority
	Goal 4 – A process for responding to and recovering from incidents is established.					
	1.	Are incidents escalated to stakeholders for input and resolution? [IMC:SG4.SP1]	2			
	2.	Are responses to declared incidents developed and implemented according to pre-defined procedures? [IMC:SG4.SP2]	3			
	3.	Are incident status and response communicated to affected parties (including public relations staff and external media outlets)? [IMC:SG4.SP3]	2			
	4.	Are incidents tracked to resolution? [IMC:SG4.SP4]	3			
	Goal 5 – Post-incident lessons learned are translated into improvement strategies.					
	1.	Is analysis performed to determine the root causes of incidents? [IMC:SG5.SP1]	3			
	2.	Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)? [IMC:SG5.SP2]	2			
	3.	Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	2			
6 Service Continuity Management						
The purpose of Service Continuity Management is to ensure the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.						
	Goal 1 – Service continuity plans for high-value services are developed.					
	1.	Are service continuity plans developed and documented for assets required for delivery of the critical service? [SC:SG3.SP2]				
		People	1			
		Information	1			
		Technology	1			
		Facilities	1			
	2.	Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2]	1			
	3.	Are staff members assigned to execute specific service continuity plans? [SC:SG3.SP3]	1			
	4.	Are key contacts identified in the service continuity plans? [SC:SG2.SP2]	1			
	5.	Are service continuity plans stored in a controlled manner and available to all those who need to know? [SC:SG3.SP4]	1			
	6.	Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1]	1			

	Service Continuity Management Practice Implementation Stages		Implementation Stage	CRR Re-sponse	Gap Stage	Priority
	Goal 2 – Service continuity plans are reviewed to resolve conflicts between plans.					
	1.	Are plans reviewed to identify and resolve conflicts? [SC:SG4.SP2]	2			
	Goal 3 - Service continuity plans tested to ensure they meet their stated objectives.					
	1.	Have standards for testing service continuity plans been implemented? [SC:SG5.SP1]	2			
	2.	Has a schedule for testing service continuity plans been established? [SC:SG5.SP1]	2			
	3.	Are service continuity plans tested? [SC:SG5.SP3]	1			
	4.	Are backup and storage procedures for high-value information assets tested? [KIM:SG6.SP1]	1			
	5.	Are test results compared with test objectives to identify needed improvements to service continuity plans? [SC:SG5.SP4]	1			
	Goal 4 – Service continuity plans are executed and reviewed.					
	1.	Have conditions been identified that trigger the execution of the service continuity plan? [SC:SG6.SP1]	1			
	2.	Is the execution of service continuity plans reviewed? [SC:SG6.SP2]	1			
	3.	Are improvements identified as a result of executing service continuity plans? (SC:SG7.SP2)	1			
7 Risk Management						
The purpose of Risk Management is to identify, analyze, and mitigate risks to critical service assets that could adversely affect the operation and delivery of services.						
	Goal 1 – A strategy for identifying, analyzing, and mitigating risks is developed.					
	1.	Have sources of risk that can affect operations been identified? [RISK: SG1.SP1]	1			
	2.	Have categories been established for risks? [RISK: SG1.SP1]	3			
	3.	Has a plan for managing operational risk been established? [RISK: SG1.SP2]	2			
	4.	Is the plan for managing operational risk communicated to stakeholders? [RISK: SG1.SP2]	2			
	Goal 2 – Risk tolerances are identified, and focus of risk management is established.					
	1.	Have impact areas been identified, such as reputation, financial health, and regulatory compliance? [RISK: SG2.SP2]	2			
	2.	Have impact areas been prioritized to determine their relative importance? [RISK: SG2.SP2]	2			
	3.	Have risk tolerance parameters been established for each impact area? [RISK: SG2.SP2]	2			

		Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
	4.	Are risk tolerance thresholds, which trigger action, defined for each category of risk? [RISK: SG2.SP1]	2			
	Goal 3 – Risks are identified.					
	1.	Are operational risks that could affect delivery of the critical service identified? [RISK: SG3.SP2]	1			
	Goal 4 – Risks are analyzed and assigned a disposition.					
	1.	Are risks analyzed to determine potential impact to the critical service? [RISK: SG4.SP1]?	2			
	2.	Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks? [RISK: SG4.SP3]	2			
	Goal 5 – Risks to assets and services are mitigated and controlled.					
	1.	Are plans developed for risks that the organization decides to mitigate? [RISK: SG5.SP1]	1			
	2.	Are identified risks tracked to closure? [RISK: SG5.SP2]	3			
8 External Dependencies Management						
The purpose of External Dependencies Management is to establish processes to manage an appropriate level of controls to ensure the sustainment and protection of services and assets that are dependent on the actions of external entities.						
	Goal 1 – External dependencies are identified and prioritized to ensure sustained operation of high-value services.					
	1.	Are dependencies on external relationships that are critical to the service identified? [EXD:SG1.SP1]	1			
	2.	Has a process been established for creating and maintaining a list of external dependencies? [EXD:SG1.SP1]	2			
	3.	Are external dependencies prioritized? [EXD:SG1.SP2]	2			
	Goal 2 – Risks due to external dependencies are identified and managed.					
	1.	Are risks due to external dependencies identified and managed? [EXD:SG2.SP1]	1			
	Goal 3 – Relationships with external entities formally established and maintained.					
	1.	Have resilience requirements of the critical service been established that apply specifically to each external dependency? [EXD:SG3.SP2]	1			
	2.	Are these requirements reviewed and updated? [EXD:SG3.SP2]	3			

		Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
	3.	Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process? [EXD:SG3.SP3]	3			
	4.	Are resilience requirements included in formal agreements with external entities? [EXD:SG3.SP4]	3			
	Goal 4 – Performance of external entities is managed.					
	1.	Is the performance of external entities monitored against resilience requirements? [EXD:SG4.SP1]	3			
	2.	Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)? [EXD:SG4.SP1]	3			
	3.	Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)? [EXD:SG4.SP2]	2			
	4.	Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]	3			
	Goal 5 – Dependencies on public services and infrastructure service providers are identified.					
	1.	Are public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) identified? [EC:SG4.SP3]	2			
	2.	Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified? [EC:SG4.SP4]	1			
9 Training and Awareness						
The purpose of training and awareness is to promote awareness in and develop skills and knowledge of people in support of their roles in attaining and sustaining operational sustainment and protection.						
	Goal 1 – Cyber security awareness and training programs are established.					
	1.	Have cyber security awareness needs been identified for the critical service? [OTA:SG1.SP1]	4			
	2.	Have required cyber security skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP1]	4			
	3.	Are skill gaps present in personnel responsible for cyber security identified? [OTA:SG3.SP1]	4			
	4.	Have cyber security training needs been identified? [OTA:SG3.SP1]	4			
	Goal 2 – Awareness and training activities are conducted.					
	1.	Are cyber security awareness activities for the critical service conducted? [OTA:SG2.SP1]	4			
	2.	Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]	3			

		Service Continuity Management Practice Implementation Stages	Implementation Stage	CRR Response	Gap Stage	Priority
	3.	Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]	4			
	4.	Are awareness and training activities revised as needed? [OTA:SG1.SP3 and OTA:SG3.SP3]	4			
	5.	Have privileged users been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]	3			
	6.	Have senior executives been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]	3			
	7.	Have physical and information security personnel been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]	3			
10 Situational Awareness						
The purpose of Situational Awareness is to actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture.						
	Goal 1 – Threat monitoring is performed.					
	1.	Has responsibility for monitoring sources of threat information been assigned? [MON:SG1.SP2]	3			
	2.	Have threat monitoring procedures been implemented? [MON:SG2.SP2]	3			
	3.	Have resources been assigned to threat monitoring processes? [MON:SG2.SP3]	3			
	Goal 2 – The requirements for communicating threat information are established.					
	1.	Have internal stakeholders (such as the critical service owner and incident management staff) been identified to whom threat information must be communicated? [COMM:SG1.SP1]	3			
	2.	Have external stakeholders (such as emergency management personnel, regulatory, and information sharing organizations) been identified to whom threat information must be communicated? [COMM:SG1.SP1]	4			
	Goal 3 – Threat information is communicated.					
	1.	Is threat information communicated to stakeholders? [COMM:SG3.SP2]	3			
	2.	Have resources been assigned authority and accountability for communicating threat information? [COMM:SG2.SP3]	3			
	3.	Have resources been trained with respect to their specific role in communicating threat information? [COMM:SG2.SP3]	3			

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	April 2019	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
A Targeted Improvement Plan for Service Continuity	FA8721-05-C-0003

6. AUTHOR(S)

Andrew Hoover, Gavin Jurecko, Jeffrey Pinckard, Phillip Scolieri, Robert Vrtis

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2019-TN-002

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This technical note describes how an organization can leverage the results of a Cyber Resilience Review to create a Targeted Improvement Plan for its Service Continuity Management (SCM). An organization can use the Cyber Resilience Review (CRR) results and prioritize SCM-specific and supporting practices using a SCM improvement profile to develop a long-term plan. The suggested Targeted Improvement Plan (TIP) approach engages the organization's business continuity professionals, information technology operations management staff, and security management team (physical and cyber) to create a resilient organization. (In some organizations, it will be appropriate to engage the operational technology team as well.) The technical note includes a SCM Improvement Template that prioritizes all the CRR practices; it places a higher priority on those practices that enable service continuity. It describes how an organization can integrate the results of a recent CRR to create a prioritized list of practices the organization should consider implementing. This list informs decisions that take into account the organization's unique risk environment to develop a plan. This approach to developing and implementing a SCM program supports organization-specific, mission-focused objectives to protect and sustain a critical, cyber-dependent service during times of stress.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Cyber Resilience Review, CRR, TIP, service continuity management, SCM	27

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102