Resilience Management Through the Use of CERT-RMM and Associated Success Stories

Dr. Nader Mehravari, MBCP, MBCI
CERT Cyber Resilience Center
Software Engineering Institute
Carnegie Mellon University
nmehravari@sei.cmu.edu

***Abstract*—The CERT® Resilience Management Model (CERT-RMM), which was developed by the CERT Division at Carnegie Mellon University's Software Engineering Institute, is the most modern and comprehensive framework for managing operational resilience in a variety of organizations—small or large, simple or complex, public or private. CERT-RMM enables a structured, repeatable, and integrated method for organizations to plan, assess, manage, and sustain not only preparedness planning efforts (e.g., disaster recovery, business continuity, crisis management) but also other key operational risk management activities, such as information security and Information Technology (IT) operations. In this paper, we share practical and successful applications of CERT-RMM from a wide variety of organizations ranging from the Department of Homeland Security, to the Department of Energy, to the U.S. Postal Service, to industry giants such as Lockheed Martin.**

Keywords—resilience management; disaster recovery; operational risk management; cybersecurity; business continuity

I. INTRODUCTION

The CERT Resilience Management Model (CERT-RMM) [1-4] is an innovative and transformative way to approach the challenge of managing operational resilience in complex, risk-evolving environments. CERT-RMM is the result of years of research into the ways that organizations manage the security and survivability of the assets that ensure mission success. CERT-RMM incorporates concepts from an established process improvement community to create a model that transcends mere practice implementation and compliance. This new model can be used to mature an organization's capabilities and improve predictability and success in sustaining operations whenever disruption occurs [2].

The ability to manage operational resilience at a level that supports mission success is the focus of CERT-RMM. By improving operational resilience management processes, the organization in turn improves the mission assurance of high-value services. The success of such high-value services in meeting their missions consistently over time and in particular when stressful conditions occur is vital to meeting organizational goals and objectives [2].

In this paper, we share practical and successful applications of CERT-RMM from a wide range of organizations ranging from the Department of Homeland Security, to the Department of Energy, to the US Postal Service, to industry giants such as Lockheed Martin Corporation.

The balance of this paper is organized as follows. In Section 2, we present an overview of CERT-RMM. In Sections 3-6, we present four innovative applications of CERT-RMM as outlined in Table 1.

Section of this Paper	Organization	Program
3	U.S. Department of Homeland Security (DHS)	Cyber Resilience Review (CRR)
4	U.S. Department of Energy (DOE)	Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
5	U.S. Postal Inspection Service (USPIS)	Various
6	Lockheed Martin Corporation	Corporate Business Resiliency Initiative

Table 1: Application of CERT-RMM Presented in Sections 3-6

We end this paper by presenting our conclusions in Section 7, followed by a list of references in Section 8.

II. OVERVIEW OF THE CERT-RMM

CERT-RMM was developed by (1) studying over 800 practices for information security, business continuity, disaster recovery, and IT operations; (2) examining disaster recovery and business continuity knowledge of financial industry; (3) collaborating with high-maturity organizations; (4) examining process improvement architecture; and (5) piloting draft versions of the Model in private and government organizations.

The development of CERT-RMM was driven by factors such as

- Increasingly complex operational environments
- Siloed nature of operational risk activities
- Lack of common language or taxonomy
- Overreliance on technical approaches
- Lack of a means to measure organizational capability
- Inability to confidently predict outcomes, behaviors, and performance under times of stress

What is CERT-RMM?
• Framework for managing and improving operational resilience
• Guides implementation, management, and sustainment of operational risk management activities
• Improves confidence in how an organization manages and responds to operational stress
• Focuses on "What" not "How"
• Applicable to a variety of organizations (small or large; simple or complex; public or private)

Table 2: High-Level Description of CERT-RMM

CERT-RMM is based on a set of foundational elements, which are listed in Table 3 and further described below.

Foundational Elements of CERT-RMM
• Operational Resilience
• Operational Risk Management
• Convergence
• Organizational Construct for Resiliency Activities
• Protection and Sustainment Activities
• Institutionalization
• Lifecycle View
• Code of Practice Crosswalk

Table 3: Cornerstones of CERT-RMM

A. Operational Resilience

Operational resilience is the emergent property of an entity that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit. Disruptions come from realized risk that could be

- Natural or manmade
- Accidental or intentional
- Small or large
- Information technology or not
- Cyber or kinetic

B. Operational Risk Management

Operational risk is a form of risk affecting day-to-day business operations. It is a very broad risk category ranging from high-frequency low-impact, to low-frequency, high-impact. Operational risks are exacerbated by actions of people, systems and technology failures, failed internal processes, external events, and bad decisions. As depicted in Figure 1, operational risks are the largest subset of enterprise-wide risks.

Figure 1: Operational Risks as the Largest Subset of Enterprise Risks

C. Convergence

Convergence is a fundamental concept for managing operational resilience. For CERT-RMM purposes, convergence is defined as the harmonization of operational risk management activities that have similar objectives and outcomes [2]. These activities include

- Security planning and management
- Business continuity and disaster recovery management
- IT operations and service delivery management

Figure 2: Convergence of Operational Risk Management Activities

D. Organizational Construct for Resiliency Activities

A key aspect of services is the concept of high-value services—those that are critical to the success of the organization's mission, as depicted in Figure 3. The high-value services of the organization are the focus of the organization's operational resilience management activities. These services directly support the achievement of strategic objectives and therefore must be protected and sustained to the extent necessary to minimize disruption. Failure to keep these services viable and productive may result in significant inability to meet strategic objectives and, in some cases, the organization's mission. To appropriately scope the organization's operational

resilience management processes and corresponding operational resilience management activities, the high-value services of the organization must be identified, prioritized, and communicated as a common target for success. High-value services serve as the focus of attention throughout CERT-RMM as the means by which to establish priorities for managing risk and improving processes, given that it is not possible (nor does it make good business sense) to mitigate all risks and improve all processes. High-value services are fueled by organizational assets such as people, information, technology, and facilities [2].

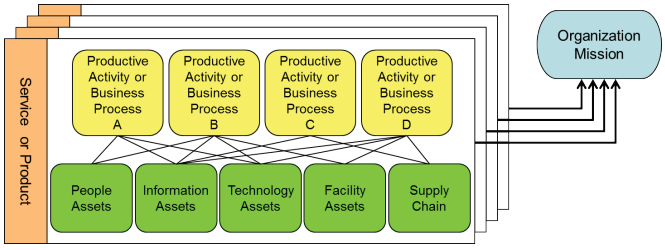

Figure 3: Organizational Context for Resilience Management

E. Protection and Sustainment Activities

An important aspect of operational resilience management is the optimization of protection and sustainment strategies and activities that minimize risk to assets and services while making efficient use of limited resources.

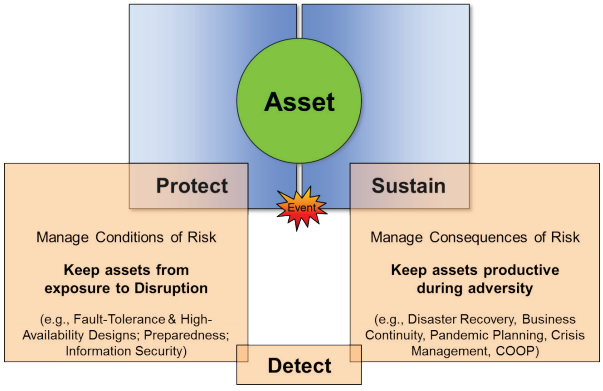

Figure 4: Protection and Sustainment Strategies

F. Institutionalization

CERT-RMM combines the two approaches of operational resilience management system and institutionalization and improvement, as depicted in Figure 5.

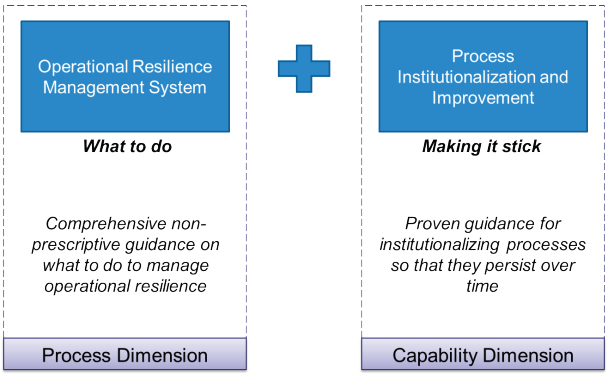

Figure 5: Institutionalization and Improvement in CERT-RMM

G. Lifecycle View

To improve and sustain an entity's operational resilience, it is not sufficient to only improve protection and sustainment activities. Resiliency should not be an afterthought; resiliency should be engineered and built-in. These concepts are present in CERT-RMM and are depicted in Figure 6.

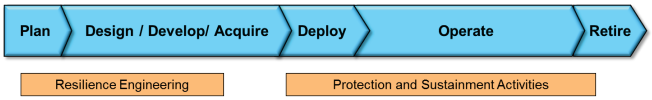

Figure 6: Lifecycle View of CERT-RMM

H. Code of Practice Crosswalk

CERT-RMM code of practice crosswalks link its practices to commonly used codes of practices and standards including

- ANSI/ASIS SPC.1-2009
- BS25999
- COBIT 4.1
- COSO ERM Framework
- CMMI
- FFIEC BCP Handbook
- ISO 20000-2
- ISO/IEC 24762
- ISO/IEC 24762
- ISO/IEC 27005
- ISO/IEC 31000
- NFPA 1600
- PCI DSS

The power of CERT-RMM comes from its unique and distinguishing features including

- Converging key operational risk management activities such as security, Business Continuity/Disaster Recovery (BC/DR), and IT operations
- Guiding the implementation and management of operational resilience activities
- Providing a descriptive rather than prescriptive approach; focuses on the "what" not the "how"
- Providing an organizing convention for effective selection and deployment of codes of practice and standards
- Guiding improvement in areas where an organization's capability does not equal its desired state
- Improving confidence in how an organization responds in times of operational stress

- Providing a baseline from which to perform assessments and appraisals
- Enabling measurements of effectiveness
- Providing a process improvement model
- Enabling institutionalization
- Providing a non- proprietary model

In the next four sections, we share practical and successful applications of CERT-RMM from a wide range of organizations ranging from the Department of Homeland Security, to the Department of Energy, to the U.S. Postal Service, to industry giants such as Lockheed Martin.

III. U.S. Department of Homeland Security (DHS) Cyber Resilience Review (CRR)

Cyber Resilience Review (CRR) is a U.S. Department of Homeland Security (DHS) program intended to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services and assets during normal operations and during times of operational stress and crises [6]. The CRR is based on CERT-RMM [4-8].

The CRR seeks to elicit the current state of cybersecurity management practices from key cybersecurity personnel: Chief Information Officers, Chief Information Security Officers, and those responsible for managing IT Security, IT Operations, and Business Continuity [6]. The CRR is a review of the overall practice, integration, and health of an organization's cybersecurity program. The CRR seeks to understand the cybersecurity management of services (and associated assets) critical for an organization's mission success by focusing on protection and sustainment practices within key areas that typically contribute to the overall cyber resilience of an organization [4-8].

Although applicable to a wide range of entities, the primary target organizations of the CRR are

- Critical Infrastructure and Key Resources (CIKR) providers
- State, local, tribal, and territorial (SLTT) governments

Goals of the CRR Program
❖ Develop an understanding of an organization's • operational resilience • ability to manage cyber risk to its critical services and its related assets (information, technology, resources, and personnel) o during normal operations o during times of operational stress and crises ❖ Improve the security posture of CIKR, state and local governments, and international partners through on-site assessment activities

Table 4: Goals of the CRR Program

The CRR incorporates a portion of CERT-RMM's 26 process areas that were identified to be most relevant to the goals and objectives of the CRR program. The CRR was developed for DHS by the same team that had defined and developed CERT-RMM at the Software Engineering Institute (SEI). As shown in Table 5, there are 10 domains in CRR. These domains represent important areas that contribute to the cyber resilience of an organization. The domains focus on practices an organization should have in place to assure the protection and sustainment of its critical service. [4-8]

CRR Domains	
AM	Access Management
CTL	Controls Management
CCM	Configuration and Change Management
VM	Vulnerability Management
IM	Incident Management
SCM	Service Continuity Management
RM	Risk Management
EXD	External Dependencies Management
TA	Training and Awareness
SA	Situational Awareness

Table 5: Domains That CRR Examines

The CRR process produces a report that summarizes observed strengths and weaknesses in each domain. This report also provides options for consideration containing general guidance or activities aimed at improving the cybersecurity posture and preparedness of an organization [6].

Benefits of CRR include providing

- An opportunity for organizations to
  - o better understand their role in critical infrastructure
  - o strengthen their cybersecurity posture
- Review of those capabilities that are most important to ensuring the continuity of critical services during times of operational stress
- Insight into an organization's cybersecurity management
- Identification of opportunities for targeted improvement
- Reduction of operational risks related to cybersecurity

IV. U.S. Department of Energy (DOE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was developed in support of a White House initiative led by the Department of Energy (DOE), in partnership with DHS, and in collaboration with industry, private-sector, and public-sector experts. The model was developed collaboratively with an industry advisory group through a series of working sessions. The model was revised based on feedback from industry experts and pilot evaluations [9-10]. The overall concept of ES-C2M2 is summarized in Table 6.

ES-C2M2 at a Glance	
Sponsor	❖ Department of Energy (DOE)
Target User Organizations	❖ All electric utilities and grid operators, regardless of ownership structure, size, or function
Challenge	❖ Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid
Objectives	❖ Strengthen cybersecurity capabilities ❖ Enable consistent evaluation and benchmarking of cybersecurity capabilities ❖ Share knowledge and best practices ❖ Enable prioritized actions and cybersecurity investments

Table 6: Overall Concept of ES-C2M2

The model is comprised of 10 domains and 4 maturity indicator levels (MILs) [9]. The overall structure of the model is depicted in Figure 7. ES-C2M2 is a dual progression model where two things are progressing across the maturity indicator levels:

1. **Institutionalization** – the extent to which the practices are ingrained in the organization's operations
2. **Approach** – the completeness, thoroughness, or level of development/sophistication of the activity

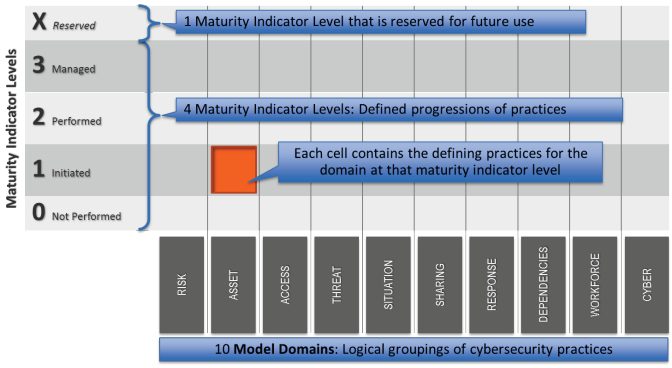

Figure 7: Overall Structure of ES-C2M2 Model

The definitions of the model's Maturity Indicator Levels are given in Table 7.|

Each of the model's 10 domains is a structured set of cybersecurity practices. Each set of practices represents the activities an organization can perform to establish and mature capabilities in the domain. For example, the Risk Management domain is a group of practices that an organization can perform to establish and mature cybersecurity risk management capability [9].

Level	Name	Description
MIL0	Not Performed	MIL1 has not been achieved in the domain.
MIL1	Initiated	Initial practices are performed, but they may be ad hoc.
MIL2	Performed	Practices are documented. Stakeholders are involved. Adequate resources are provided for the practices. Standards or guidelines are used to guide practice implementation. Practices are more complete or advanced than at MIL1.
MIL3	Managed	Domain activities are guided by policy (or other directives). Activities are periodically reviewed for conformance to policy. Responsibility and authority for practices are clearly assigned to personnel with adequate skills and knowledge. Practices are more complete or advanced than at MIL2.

Table 7: Definition of Maturity Indicator Levels (MILs)

V. Applications of CERT-RMM at the U.S. Postal System

Developing and implementing measurable methodologies for improving the security and resilience of the postal sector directly contributes to protecting public and postal employees, assets, and revenues. Such methodologies also contribute to the security and resilience of the mode of transport used to carry mail items and to the protection of the global supply chain.

During the past several years, the United States Postal Inspection Service (USPIS) has collaborated with the CERT Division at the Carnegie Mellon University Software Engineering Institute to improve the resilience of selected U.S. Postal Service (USPS) services and processes [12]. This successful collaboration has included projects dealing with

- Physical security and aviation screening for international mail
- Export screening
- New USPS product security
- Authentication portal services
- Measurement and monitoring of risks associated with fraud
- Improved processes for investigative response to network security incidents
- Development of mail-specific resilience management principles and practices for mail induction, transportation, delivery, and revenue assurance

CERT-RMM and its companion diagnostic methodologies have served as the foundational tool for the collaboration between the USPIS and the CERT Division. CERT-RMM is a capability-focused model for process improvement that reflects best practices from industry and government for managing operational resilience across the domains of security management, business continuity management, and aspects of information technology operations management. Principles and practices in the model focus on improving the organization's management of key operational resilience activities. These improvements enable high-value services to meet their missions consistently and with high quality, particularly during times of stress and disruption.

Safety, security, and resiliency of international postal and transportation critical infrastructure are vital to the global supply chain that enables worldwide commerce and communications. Security on an international scale continues to fail in the face of new and complex threats. This reality, together with the ever-increasing complexity of the global supply chain, calls for new and innovative approaches. Owners and operations of critical postal and transportation operations need new methods to identify, assess, and mitigate security risks and gaps in the most efficient and expedient manner possible.

The USPIS, in collaboration with the CERT Division at the SEI, have developed, implemented, and successfully used an innovative physical security risk assessment method to assess and identify gaps in the security of international mail processing centers and similar transportation processing facilities. This assessment method and its associated field instrument are designed to be

- **Repeatable**: able to be used consistently by different independent teams in the same situation to acquire the same results
- **Cost effective and scalable**: economic and functional for all locations, regardless of size or capability
- **Accurate**: evidence-based and derived from international standards so that results can be relied upon by the international community (e.g., UPU (Universal Postal Union), ICAO (International Civil Aviation Organization), TSA (Transportation Security Administration), and airlines)
- **Meaningful**: generates results that can easily be acted on by owners and operators of the assessed processing facilities
- **Transparent**: (to be published) publicly available and can be used for self-assessment

The USPIS has demonstrated these characteristics through use of the field instrument in a variety of international settings. Moreover, since the subject methodology takes advantage of international UPU standards as reference criteria, it is expected that the appraisal method will be used by the international community to evaluate the security of postal administrations around the world. In addition, the method and instrument can be tailored and applied to other types of critical transportation services, including those that move people (such as metropolitan area transit systems), and air, ground, and sea transportation of goods.

VI. Application of CERT-RMM at Lockheed Martin

Lockheed Martin Corporation has collaborated with the SEI on the application of the CERT-RMM to improve Lockheed Martin's corporate-wide business continuity, IT disaster recovery, crisis management, and pandemic planning activities [13].

Lockheed Martin's Corporate Business Resiliency Strategic Initiative defines Business Resiliency Management (BRM) as the practice of planning, developing, executing, and governing activities to ensure that an enterprise

- Identifies and mitigates operational risks that can lead to business disruptions before they occur
- Prepares for and responds to disruptive events (natural or man-made, accidental or intentional) in a manner that demonstrates command and control of incident response
- Recovers and restores mission-critical business operations following a disaster within acceptable time frames

Lockheed Martin has used CERT-RMM in a variety of ways. For example, it has been used as an enterprise-wide common ruler to answer such questions as

- Assessment of current levels of competencies
  - Where are we now? How good are we now?
  - A consistent and common "ruler"
  - Assessment by self, internal third party, external third party
- Guidance for future direction and investments
  - Where do we want to be? How well do we want to get?
  - Setting objectives
  - Determining the investments required to reach the next/desired level
  - Realization that it is not necessary for all organizations to reach the most top level
- A measure of progress towards the desired goal
- Assurance that the plans and processes continue to evolve with the needs of the organization
  - How do we stay there?

At Lockheed Martin CERT-RMM is also

- Contributing to the common business resiliency taxonomy and nomenclature
- Serving as a contributing reference model for the integrated business resiliency framework
- Serving as a maturity model to gauge the preparedness posture of individual business entities and/or the enterprise as a whole in the areas of disaster recovery and business continuity
- Serving as a mechanism to reveal insights about existing policies and guidelines

- Serving as a guiding tool in the developing of new command media
- Serving as a means to communicate key harmonization and convergence across business resiliency and information security

VII. SUMMARY

CERT-RMM [1-4] enables a structured, repeatable, and integrated method for organizations to plan, assess, manage, and sustain preparedness planning efforts and operational risk management activities. Successful experiences from applications in the four organizations summarized in this paper demonstrate CERT-RMM's capability to be easily tailored to the needs and nature of a variety of organizations. Moreover, the cases summarized in this paper reveal CERT-RMM's ability to be applied across organizational boundaries and across preparedness planning domains.

VIII. REFERENCES

[1] Richard A. Caralli, Julia H. Allen, and David W. White. *CERT Resilience Management Model (RMM): A Maturity Model for Managing Operational Resilience*, Addison-Wesley Professional, 1st edition, December 4, 2010.

[2] Richard A. Caralli, Julia H. Allen, Pamela D. Curtis, David W. White, and Lisa R. Young, *CERT® Resilience Management Model, Version 1.0, Improving Operational Resilience Processes* (CMU/SEI-2010-TR-012). Software Engineering Institute, Carnegie Mellon University, 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9479

[3] Resilience Management. Software Engineering Institute, Carnegie Mellon University, 2014. http://www.cert.org/resilience/

[4] Julia H. Allen and Noopur Davis. *Measuring Operational Resilience Using the CERT® Resilience Management Model* (CMU/SEI-2010-TN-030). Software Engineering Institute, Carnegie Mellon University, 2010, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9401

[5] Department of Homeland Security. "Cyber Resilience Review Frequently Asked Questions," 2011. http://thielst.typepad.com/files/crr-faq_20111024-1.pdf

[6] Department of Homeland Security. *Cyber Resilience Review*,2012. http://www.ahrmm.org/ahrmm/news_and_issues/issues_and_initiatives/files/ahrmm_cyber_resilience_review_032712.pdf

[7] Bradford J. Willke. "Securing the Nation's Critical Cyber Infrastructure," April 14, 2010. https://ics-cert.us-cert.gov/icsjwg/presentations/spring2010/01%20-%20Case%20studies%20-%20Bradford%20Willke.pdf

[8] Samuel A. Merrell, Andrew P. Moore, and James F. Stevens. "Goal-Based Assessment for the Cybersecurity of Critical Infrastructure," IEEE, 2010. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5655090

[9] Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.0, May 2012. http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf

[10] Office of Electricity Delivery & Energy Reliability. "Electricity Subsector Cybersecurity Capability Maturity Model," 2014. http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model

[11] National Electric Sector Cybersecurity Organization. http://www.linkedin.com/groups/ESC2M2-3737063.S.120834518

[12] Greg Cragg and Julia H. Allen. U.S. Postal Inspection Service Use of the CERT Resilience Management Model (podcast). Software Engineering Institute, Carnegie Mellon University, 2012. http://www.cert.org/podcast/show/20120821crabb.html

[13] David, William, Mehravari, Nader, and White, W. David. Application of the CERT Resilience Management Model at Lockheed Martin, 2011 SEPG North America Conference. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=19352