# CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

## How Resilient Is My Organization?

**Key Message:** Use the CERT® Resilience Management Model (CERT®-RMM) to help ensure that critical assets and services perform as expected in the face of stress and disruption.

**Executive Summary**

The CERT Resilience Management Model is a capability model for managing operational resilience. It has two primary objectives

- Establish the convergence of operational risk and resilience management activities such as security, business continuity, and aspects of IT operations management into a single model.
- Apply a process improvement approach to the management of operational resilience through the definition and application of a capability level scale that expresses increasing levels of process maturity.

In this podcast, Rich Caralli, the technical manager for CERT's Resilience Enterprise Management team, and Dave White, the team lead for the CERT Resilience Management Model, provide an update on CERT-RMM, version 1.1, the RMM book, and plans for the coming year.

---

**PART 1: RESILIENCE: THE CONVERGENCE OF SECURITY, BUSINESS CONTINUITY, AND IT OPERATIONS**

**Why Resilience?**

The ultimate goal of security is not security for security's sake or to stop or prevent something; it's resilience, to enable the mission of the organization.

Security is one means to achieving resilience. We cannot prevent all threats and all vulnerabilities. We must take an interdisciplinary approach that limits impact. And we need to consider both protection (be proactive) and sustainability (react and recover).

A threat or vulnerability only matters if it disrupts something important. An organization needs to focus their security, business continuity, and IT operations efforts on carrying out their mission in the face of ever-changing risk environments.

**The Evolution of CERT-RMM**

The original purpose of CERT-RMM was to identify key activities that organizations needed to perform to survive in the face of stress and disruption.

Over the past six years, the purpose of the model has evolved to one of transforming a community or an industry to a resilience view. This means moving from adhoc, get-lucky activities to being able to determine your organization's capability for handling stress, with justified confidence and predictability.

**Scope, Audience, and Application**

CERT-RMM

- presents a converged view of three disciplines: security, business continuity/disaster recovery, and aspects of IT

operations management
- is intended for anyone interested in better assuring the mission of high-value services and associated assets
- is scalable to any size of organization
- includes a crosswalk that provides traceability to many commonly used codes of practice such as the ISO 27000 series, COBIT, and ITIL
- extends the use of models such as the SEI's CMMI into the operations phase of the software and system asset life cycle

---

**PART 2: STRUCTURE AND USE**

**Structure**

CERT-RMM includes 26 process areas (PAs) organized into 4 categories as follows:

- Engineering (6 PAs): identify, protect, and sustain assets
- Enterprise Management (7 PAs): high-level, enterprise-wide activities necessary for managing resilience
- Operations (9 PAs): ongoing, day-to-day activities for managing resilience
- Process Management (4 PAs): implement, measure, monitor, and improve resilience processes

Each PA consists of a set of specific goals (SGs) and specific practices (SPs). Across all 26 PAs, there are 94 specific goals and 251 specific practices. In addition, each PA has 3 generic goals (GGs) and 13 generic practices (GPs).

The GGs and GPs define capability levels 0, 1, 2, and 3. There are currently 4 levels of capability based on observed practice; more levels may be added in the future.

The architecture of CERT-RMM is very similar to CMMI. That said, CERT-RMM only includes a continuous representation (capability level is chosen by PA). It does not include a prescriptive path through all process areas in the model (a staged representation).

**CERT-RMM vs. Other Maturity Models: The Differentiators**

The capability levels in CERT® Resilience Management Model (CERT®-RMM) that describe how well a process has been institutionalized have an empirical basis (research, application, and observation); they are not arbitrary.

The extent of institutionalization helps determine how well a practice will "stick" during times of stress.

CERT-RMM draws from the SEI's experience in and application of CMMI.

**Applying CERT-RMM**

Today, many organizations are using the model for benchmarking and gap analysis, to evaluate current activities, and to plan for improving their resilience posture.

CERT-RMM is also being used to:

- improve information security activities and compliance responsibilities associated with these
- improve IT operations activities
- improve business continuity and disaster recovery operations at the policy level
- evaluate critical infrastructure protection activities
- develop a federated view of operational risk
- establish a baseline for return on investment related to resilience
- protect electronic health records

---

## PART 3: MAKING THE BUSINESS CASE

### Business-Based Arguments for Improving Operational Resilience

CERT-RMM is a reference model. Organizations can pick and choose their areas of greatest interest, starting by making a small investment of time and resources. For example, you can use the incident management process area to learn about practices performed by high maturity organizations. Read a chapter and ask the question, “How closely does the process we use align with this?”

Process improvement requires a stimulus for change, for example, improve sales, reduce costs, and become more efficient. The quality argument also applies here: investments in high product quality, over time, pay for themselves.

Improving the processes for managing resilience should improve organizational effectiveness during times of stress and avoid costly impacts. It should also reduce redundant efforts resulting from siloed security, continuity, and IT operations activities.

Current investments in IT, security, and resilience (which are often considerable) can produce a much better return with resilience in mind.

---

## PART 4: GETTING STARTED; UPCOMING CERT-RMM PRODUCTS

### Given 26 Process Areas, Where Do I Start?

Once people understand the 26 process areas and the model, they generally know where they want to start – which is generally what brought them to CERT-RMM in the first place.

To get started

- Peruse the model. Each PA has a one to two sentence purpose statement. Read these first and pick those that are of greatest interest based on your improvement objective.
- Pick which parts of the organization will be the target for improvement. This is often based on some organizational objective and the sponsor for the improvement activity.
- Select a specific process area or goals and practices within several process areas.

This process is called scoping.

### Sponsor Roles

Roles that tend to have greatest interest in improvement using CERT-RMM include managers responsible for business continuity, chief information officers, or chief information security officers.

Senior executives in these operational risk and resilience areas, and those in governance and management roles, need to be able to answer key questions such as "Are we secure?" and "Are we resilient?" They need to be able to express

- justified confidence (with a defensible basis)
- indicators of success
- indictors that investment dollars are well spent
- indicators that the organization is benefiting from implementing better practices

CERT-RMM provides this level of characterization.

### Alleviating Pain Points

Others who are interested in using CERT-RMM include practitioners who are seeing the same incidents over and over

again, and who are following established standards and still experiencing security breaches.

Codes of practice are well and good but they often do not get to the root cause of the problem.

**What's Next for CERT-RMM?**

Here are some of the plans for CERT-RMM in the coming year:

- CERT-RMM version 1.1 available in book form from Addison-Wesley. The book includes implementation guidelines such as targeted improvement roadmaps and process areas for meeting a specific improvement objective.
- An updated CERT-RMM Crosswalk to standard codes of practice. The updated Crosswalk will cover common NIST practices and DIACAP.
- A range of appraisal methods and the ability to become an apprentice appraiser and a licensed appraiser. CMMI-certified appraisers will be able to fast track obtaining a CERT-RMM credential.
- Two new roles include the CERT-RMM coach (for leading organizational improvement) and navigator (using a new method called Compass to conduct a self-administered health check at a low initial investment cost).
- Resilience measurement and analysis, focused on determining if improving resilience processes does indeed make an organization more resilient.
- Applying CERT-RMM in new domains such as critical infrastructure protection, electronic health records, and software and systems resilience during development.

**Resources**

CERT Resilience Management Model website.

Caralli, Richard; Allen, Julia; White, David. *The CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2010.