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

Insights from the First CERT Resilience Management Model Users Group

Key Message: Implementing CERT-RMM requires well-defined improvement objectives, sponsorship, proper scoping and diagnosis, and defined processes and measures.

Executive Summary

The CERT Resilience Management Model (RMM) Users Group (RUG) Workshop Series was originally conceived as a means to help CERT-RMM users progress in their adoption of the model and practice using it after taking the three-day Introduction to CERT-RMM course.The workshop is also intended to help CERT staff members understand the requirements necessary to implement CERT-RMM and develop materials that will help users put CERT-RMM practices into action on their specific improvement projects.

In this podcast, Lisa Young, a senior engineer with CERT's Cyber Resilience Center, discusses the first RUG that was conducted from March 2011 through February 2012. A description of this workshop series is available as an SEI technical note.

PART 1: MEMBERS, PREPARATION, SCOPING

RUG Purpose and Structure

The RUG was developed to address the following questions, raised by those starting to use the CERT-RMM model:

- How do I actually use and implement the model?
- What do I do with the model?
- How do I use the model to make my organization more resilient?

RUG members come with a business problem and identify and implement a selected set of CERT-RMM practices that will help them improve. The RUG is a hands-on experience in applying the model.

The RUG takes place over 12 calendar months. It is a series of four 2-day workshops with 4 to 5 participating organizations, each of whom have 2 to 3 participants.

Members

Member organizations for the first RUG workshop included:

- Carnegie Mellon University Information Security Office (joined at Workshop 2)
- Discover Financial Services
- Lockheed Martin Information Systems & Global Solutions
- United States Postal Inspection Service
- CERT Resilience Enterprise Management (REM) Team (joined at Workshop 2)

Preparation

Workshop members prepared for the RUG by:

- attending the Introduction to CERT-RMM course
- participating in interviews to communicate their expectations

- identifying a business problem to use as the basis for a defined improvement objective on which they could make progress over 12 calendar months

The RUG was tailored to the needs and interests of participating members.

The diversity of the sectors represented by the members was regularly mentioned as valuable. Even with this diversity, members had many common problems, particularly in responding to incidents and working with external providers and supply chain partners.

Scoping

A big challenge throughout the workshop series was understanding and selecting the CERT-RMM model scope (process areas, goals, practices) that most directly applied to the business problem each member team was addressing.

Organizational scoping is also critical, specifically to identify sponsors of improvement projects and their span of control.

Key scoping questions that were discussed included:

- What, realistically, can an organization expect to get done in 12 calendar months?
- Is the improvement project within the sponsor's span of control?
- Which parts of the business need to be involved?

Scoping was revisited often throughout the RUG. Even though the initial inclination is to include many CERT-RMM process areas (there are 26), members were advised to make their model scope as narrow as possible, to be able to make progress and a positive impact.

In addition, matching the model scope to the member team's (or sponsor's) span of control (authority, responsibility to enact improvements) increases the likelihood of success.

Diagnosis

Questions we discussed to help determine a member organization's current state included:

- What kind of diagnosis should members perform?
- Is the diagnosis an in-depth, evidentiary appraisal where evidence is collected to confirm that practices are being performed?
- Is the diagnosis more lightweight to obtain a quick health check?
- What type of diagnosis best fits with each member's defined model scope?

Model Scoping Example

An example of narrowing model scope is to focus in on incident escalation (process for escalating, when to escalate, to whom) instead of taking on the entire incident management process, which has 15 practices).

PART 2: DIAGNOSIS, PROCESS DEFINITION, MEASUREMENT

Diagnosis Round 2

For organizations new to model adoption and process improvement, one approach for effective diagnosis is to connect resilience practice diagnosis to something that is already in place such as a compliance process (evidence of controls, documentation).

For organizations with a process improvement group and users of Six Sigma and Lean Six Sigma, one approach is to

integrate resilience practice diagnosis into these existing processes.

When conducting diagnosis, it is important to have a wide range of data collection objectives and interview a variety of people to determine the current state of practice implementation.

CERT-RMM Compass

At the SEI, the evidence-based appraisal method used in concert with CMMI (Capability Maturity Model Integration) is called SCAMPI (Standard CMMI Appraisal Method for Process Improvement). This is a large, labor intensive form of diagnosis.

For CERT-RMM, we also wanted to have a "quick health check" form of diagnosis that did not require a great deal of evidentiary data collection. Compass is a questionnaire-based survey that has a set of questions and multiple-choice answers for each CERT-RMM process area specific goal and practice.

All members used Compass between workshops 2 and 3 to conduct their diagnosis.

Defining Implementation-Level Processes

Defining processes at a level at which they can be implemented is essential for having a standard, repeatable method for executing, for example, incident escalation. Defined processes specify the "how" that matches the model "what."

Another benefit of having a defined process is that it provides the context for essential measurement points to determine if improvements are occurring as intended.

Staying with the incident escalation example, the model states that you should escalate high-profile incidents to key stakeholders. But it is silent on how to actually do this. Questions addressed by a defined process would include:

- How does escalation happen?
- What actions are taken?
- What happens first, second, third?
- Who does what (define roles)?

The benefits of a defined process include:

- everyone knows what the process is and can follow it. This helps avoid adhoc, "hair on fire" behaviors during a disruptive event.
- avoiding mistakes
- collecting the evidence necessary for law enforcement and insurance purposes
- collecting lessons learned to avoid repeating ineffective actions
- resolving disconnects, for example, between the vulnerability management staff and the incident management staff

Prioritizing Improvement Actions

Criteria for prioritizing the findings and need for action that result from diagnosis include:

- sponsorship and span of control
- understanding what is not working with the current process
- the extent to which the process is used repeatably throughout the organization
- the process lifespan (longer is better)
- the extent to which the process must be done consistently and in exactly the same way every time it is executed (for example, configuring a laptop, desktop, or server)

PART 3: LESSONS LEARNED AND WORKSHOP IMPROVEMENTS

Lessons Learned

As members conducted improvement actions between each workshop, they identified approaches that worked well and that were less effective – for diagnosis, process definition, sponsorship, and other aspects.

Members gained a much greater understanding of what is required to implement the model and how to apply it to additional business problems beyond the one they tackled in the RUG.

For members with a mature process improvement group, they were able to expand their scope to address resilience.

Lisa and her colleagues who lead the RUG benefited from lessons learned on the CERT REM improvement project. They used this effort to anticipate the methods and challenges that RUG members might face, in advance of each workshop.

Workshop Improvements

Members identified a wide range of improvements for future workshops, which are described in the workshop series technical note.

Resources

Reports and Books

- Allen, Julia & Young, Lisa. *Report from the First CERT-RMM Users Group Workshop Series* (CMU/SEI-2012-TN-008). Carnegie Mellon University: Software Engineering Institute, April 2012.
- Caralli, Richard; Allen, Julia; White, David. *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011.

Courses

- CERT Resilience Management Model (CERT-RMM) Users Group Workshop Series
- Introduction to the CERT Resilience Management Model course

Websites

- CERT-RMM website
- CERT-RMM measurement and analysis