Software Engineering Institute
Carnegie Mellon University

CERT-RMM CAPABILITY APPRAISALS

Determine and improve your organization's operational resilience.

Managing operational *resilience* is a challenge that involves managing *risks* in complex environments. Because of technology and other factors, these environments (and corresponding threats and vulnerabilities) are continuously changing. You must be prepared to not only address the events you knows about, but also unforeseen events that might occur.

Organizations with lower levels of process capability and maturity tend to operate in an ad-hoc way that depends on heroics and fortunate circumstances. Organizations with higher levels of process capability and maturity operate in a way that improves their potential for managing operational resilience regardless of the risk environment. Therefore, knowing your organization's current level of process capability and maturity helps you determine its potential.

A CERT-RMM appraisal rates your organization's process capability and maturity, determining how well it's prepared to manage its operations in a changing risk environment.

About CERT-RMM Capability Appraisals

CERT-RMM appraisals are conducted by SEI-authorized appraisers who are trained in CERT-RMM and its appraisal methodology. Your organization's personnel participate in the appraisal by participating in interviews, supplying process artifacts (such as documents), facilitating process observations, analyzing findings, and drawing conclusions. How involved your organization's personnel are in an appraisal depends on the appraisal's scope. After the appraisal, your organization owns the appraisal results and can use them however it sees fit.

SEI-authorized appraisers objectively review organizations using CERT-RMM's processes and practices. You can request such an appraisal for your organization or for another one (e.g., a business partner or supplier) to examine its abilities. Either way, the appraisal provides a foundation for the long-term process improvement of the appraised organization.

A CERT-RMM appraisal provides insight into

- the current state of your organization's processes for managing operational resilience
- your organization's process strengths and weaknesses
- opportunities for improvement relative to the CERT-RMM
- potential value of improvements
- ways to prioritize improvement activities

Unlike assessments, audits, or evaluations in the security, business continuity, or IT domains, a CERT-RMM appraisal helps you understand your organization's level of capability by examining its process maturity. Further, most practice-based assessments focus on how well an organization meets a prescribed practice at a point in time; such an approach fails to evaluate whether an organization can sustain an adequate level of performance after the assessment concludes.

In contrast, a CERT-RMM appraisal helps you determine not only whether your organization is doing the right things now, it also determines whether your organization is capable of sustaining an acceptable level of performance during times of stress and over the long run.

Scope

Because you can appraise individual CERT-RMM process areas, an appraisal involves determining

- the *model* scope: the CERT-RMM process areas included in the appraisal
- the *organizational* scope, the parts or levels of the organization to be appraised (the enterprise, a line of business, one or more operating units, a specific project, etc.)

Both the model and the organizational scopes are determined during an appraisal workshop that considers criteria such as the organization's reasons for performing the appraisal, its process improvement objectives, its resilience strategy, the regulatory and compliance environment, and specific threats or risks of concern to the organization.

Benefits of the Appraisal

Besides using appraisal results to improve processes and set performance targets, your organization can use the results of a CERT-RMM appraisal to characterize its competency for managing operational resilience. For your customers, appraisal results can communicate confidence in creating a resilient partnership that can survive business and operational events. As appraisals are performed on other organizations in your core industry, you can use appraisal results to benchmark your organization's performance and compare it to your peers' results.

Improving processes can eliminate redundancies, streamline compliance activities, and increase efficiency. Appraisal results are an objective means of communicating your organization's process capability and maturity with respect to resilience. If your organization provides services to other organizations, you can share your appraisal results with potential business partners to help increase your organization's business and ability to secure contracts.

If you are new to process improvement based on a model like the CERT-RMM, you may find a less formal assessment activity to be a more appropriate place to start. Request one of our lightweight and agile appraisal methods and we will help you determine the right appraisal to use for meeting your objectives.

Learn More

Listen to Kevin Dillon and Matt Butkovic discuss how participating in a Cyber Resilience Review allows critical infrastructure owners and operators to compare their cybersecurity performance with their peers: www.cert.org/podcasts/podcast_episode.cfm?episodeid=70278.

On LinkedIn, search for *CERT Resilience Management Forum* to join our experts and others to discuss resilience management.

Take the Next Step

Contact us to learn more about CERT-RMM appraisals, become a licensed CERT-RMM appraiser, or arrange for a CERT-RMM appraiser to perform an appraisal in your organization.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0004380