

CERT Resilience Management Model (CERT-RMM) v1.2

CERT-RMM is a process-improvement framework for assessing and improving operational resilience, risk management, and incident response.



What it is

CERT Resilience Management Model (CERT-RMM) is a process improvement framework that helps organizations assess, manage, and improve their operational resilience in the areas of cybersecurity, risk management, and business continuity. The framework provides structured guidance for integrating risk and resilience activities across people, processes, technology, and assets to strengthen an organization’s ability to withstand and recover from threats and disruptions.

CERT-RMM is published by the Software Engineering Institute (SEI) at Carnegie Mellon University and is utilized by private and public sector organizations seeking to enhance the maturity of their operational resilience practices. The model covers domains such as incident management, asset management, risk assessment, service continuity, and compliance oversight, making it relevant to organizations facing complex regulatory and cybersecurity environments.

At a glance

PUBLISHER Carnegie Mellon University Software Engineering Institute (SEI)	TYPE Framework	VERSION CERT-RMM v1.2
EFFECTIVE 2015	DOMAIN Operational Resilience	FAMILY Other
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY High

Source: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084>

Why it matters

How SmartSuite supports CERT-RMM

Resilience Process Areas Library

Organize CERT-RMM process areas with owners and operational requirements.

Critical Services and Dependencies

Define critical services, assets, and dependencies with resilience requirements.

Response and Recovery Management

Manage response, recovery, and service continuity tasks with full traceability.

Assessments and Improvement Plans

Track maturity assessments, corrective actions, and continuous improvement roadmaps.

Evidence and Assurance Readiness

Centralize proof for governance, monitoring, and operational resilience practices.

Critical Services Readiness and Improvement Reporting

Report readiness, gaps, and improvements across critical services.

Common framework mappings

Official resources

CERT-RMM Version 1.2

Provides comprehensive guidance for implementing the CERT Resilience Management Model.

resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

Frequently asked questions

What is CERT-RMM used for?

CERT-RMM is a process improvement framework designed to help organizations assess, manage, and enhance their operational resilience in areas such as cybersecurity, risk management, and business continuity. It provides structured guidance to integrate and mature risk and resilience practices across people, process, technology, and assets.

Is CERT-RMM certifiable or required by regulators?

CERT-RMM is not a certifiable standard and is generally not mandated by regulators; rather, it serves as a best-practice reference model. Organizations use it to benchmark and improve operational resilience and to demonstrate due diligence in regulatory compliance contexts.

Who should use CERT-RMM and what is its scope?

CERT-RMM is applicable to both public and private sector organizations seeking to strengthen their resilience against cyber, operational, and physical threats. Its scope covers 26 process areas within Enterprise Management, Engineering, Operations, and Security domains.

What are the key concepts or artifacts required by CERT-RMM?

Key concepts in CERT-RMM include process areas, maturity levels, risk registers, asset inventories, and incident response procedures. Organizations are expected to document controls and create artifacts such as policies, plans, and compliance evidence as part of their resilience management activities.

How is CERT-RMM implemented in practice?

Organizations implement CERT-RMM by first assessing current capabilities relative to the model's process areas, mapping existing controls, identifying gaps, and developing actionable improvement plans. Ongoing reviews and process improvements are integral to aligning operations with CERT-RMM objectives.

How does CERT-RMM relate to other frameworks like NIST or ISO?

CERT-RMM is complementary to frameworks such as NIST and ISO 27001; its structured approach helps organizations harmonize governance, risk, and compliance requirements. CERT-RMM can be integrated into broader compliance programs, supporting alignment and audit readiness across multiple standards.

What are the ongoing compliance requirements when using CERT-RMM?

Ongoing compliance with CERT-RMM requires regular process reviews, continuous monitoring of risk and control effectiveness, incident response testing, and meticulous record keeping for audits. Organizations should sustain policy governance and track progress against defined maturity objectives.

How would SmartSuite support CERT-RMM?

SmartSuite supports CERT-RMM by providing modules for documenting and mapping controls to process areas, maintaining risk and asset registers, and tracking compliance status. The platform enables collection of evidence, workflow automation for remediation, and produces dashboards for real-time reporting and audit readiness, streamlining compliance and resilience management.

License included / downloadable: Yes CERT-RMM documentation is published by Carnegie Mellon University's SEI and is publicly available through official SEI resources.

Full framework page and mappings: smartsuite.com/frameworks/cert-rmm-cert-resilience-management-model-v1-2