Carnegie Mellon University
Software Engineering Institute

Cyber Risk Management

A Resilience Approach to Cybersecurity

YOUR ORGANIZATION CANNOT ANTICIPATE EVERY DISRUPTION or prevent every cyber attack. However, you must be able to anticipate and respond to changes in your risk environment at a moment's notice and be ready to continue operations and meet your mission when disruptions occur.

To accomplish this continuity of operations, you must take a resilience approach to cybersecurity—an integrated, holistic way to manage security, business continuity, disaster recovery, and IT operations—in the context of your business mission and strategy.

About

The CERT Cyber Risk Management team enables organizations to manage their operational risks and ensure mission success by conducting cybersecurity research; designing and developing models, tools, and techniques; and deploying capabilities that improve their security and resilience posture.

Our research encompasses all the aspects of planning, integrating, executing, and governing operational resilience.

Our work helps organizations ensure that they can identify and mitigate operational risks that could lead to service disruptions before they occur, prepare for and respond to disruptive events (realized risks) in a way that demonstrates command and control of incident response and service continuity, and recover and restore mission-critical services and operations after an incident within acceptable timeframes.

As a trusted partner, the Cyber Risk Management team of the Software Engineering Institute's CERT Division enables your organization to apply cyber risk and resilience management models and methods to assess and improve your operational resilience, manage operational risks, define meaningful metrics, and ensure mission success. We also provide education and training in cyber risk and resilience management to enhance your cyber workforce capabilities.

Get Started Today

The Cyber Risk Management team conducts research in several exciting areas and has developed solutions to support your organization's improvement efforts. Collaborate with us, use our tools, participate in our training, request an appraisal, explore our digital library, sponsor research and development, or attend an event. For more information, contact us at **info@sei.cmu.edu**.

Key Capabilities

Development — We Understand Structure. We design, customize, and deploy frameworks and models to improve organizational security posture.

Implementation — We Understand Use. We assist organizations through a structured approach to support adoption, develop plans, and set improvement goals and targets.

Operation — We Understand Improvement. We provide tools and methods to measure the capabilities, identify improvement gaps, and enable data-driven decisions.

Areas of Research

Operational Resilience Management

Operational resilience is an organization’s ability to prevent disruptions to its mission from occurring, continue to meet its mission if a disruption does occur, and return to business as usual after the disruption is managed. We define, validate, and make sense of frameworks and practices to balance actions that protect assets with actions that sustain services and operations, striving for the right mix to strengthen overall cybersecurity posture and meet the business mission.

Security Metrics and Risk Measurement

We research, design, and develop measurement and analysis methods to enable organizations to develop meaningful metrics and plan their use in data-driven decision making.

Governance and Capability Development

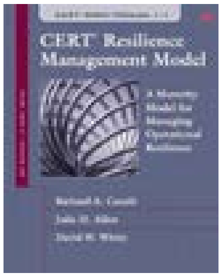
We support organizations in identifying and implementing the business processes they need to raise cybersecurity to an enterprise governance level. We define how organizations can identify their cyber workforce capabilities and their path to mature their operational resilience workforce.

Cyber Risk Management

We build roadmaps that assist organizations in improving their operational risk management capabilities, integrating with larger enterprise risk management (ERM) efforts, and achieving compliance program efficiencies.

Critical Infrastructure Resilience

We define how IT and operational technology can be combined to enable critical infrastructure decision makers to better manage operational risk.



The CERT Resilience Management Model is the foundation for a process improvement approach to operational resilience management.

Version 1.2 of CERT-RMM was published in February 2016 and is available for free download on the SEI website (**resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084**).

Solutions

Collaborating with our stakeholders, we identify and solve problems with comprehensive solutions such as the following.

CERT Resilience Management Model (CERT-RMM) is a capability-focused maturity model for process improvement that reflects best practices across the domains of security management, business continuity management, and aspects of IT operations management. An organization can use the model to establish its current level of capability in managing resilience, set goals and targets, and develop plans to close identified gaps.

Cybersecurity Capability Maturity Model (C2M2) is a CERT-RMM derivative that helps organizations evaluate and improve their cybersecurity capabilities. The model defines a set of industry-vetted cybersecurity practices and an evaluation tool that enables benchmarking of performance against those practices. There are variants of C2M2 designed specifically for the Electricity Subsector (ES-C2M2) and the Oil and Natural Gas Subsector (ONG-C2M2).

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a suite of tools, techniques, and methods for risk-based information security assessment and planning. The OCTAVE method is used to assess an organization’s information security risks.

Smart Grid Maturity Model (SGMM) is a framework for guiding utility industry transformation. Utilities can leverage this management tool to plan their transformation, prioritize their actions, and measure their progress as they move toward the realization of a smart grid.

About the CERT Division

The CERT® Division of Carnegie Mellon University’s Software Engineering Institute studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu