Carnegie Mellon
Software Engineering Institute

CERT® Resiliency Engineering Framework

The CERT® Program of the Software Engineering Institute (SEI) at Carnegie Mellon University is developing a Resiliency Engineering Framework to help organizations improve their security and sustainability processes. This document provides answers to a list of commonly asked questions about the project and the framework.

What is operational resiliency?

Operational resiliency describes the organization's ability to adapt to and manage risks that emanate from day-to-day operations. Organizations that have resilient operations are able to systematically and transparently cope with disruptive events so that the overall ability of the organization to meet its mission is not affected. Traditional activities such as security and business continuity are focused on sustaining operational resiliency.

What is resiliency engineering?

Resiliency engineering is the process by which an organization designs, develops, implements, and manages the protection and sustainability of business-critical services, related business processes, and associated assets (people, information, technology, and facilities). Simply put, resiliency engineering means establishing resiliency requirements and using them as the basis for building resiliency into business-critical processes, services, and assets to ensure they operate as intended and expected.

How does this differ from security or business continuity management?

Neither security nor business continuity activities alone can bring about operational resiliency. Instead, operational resiliency *emerges* when security and business continuity activities are collectively focused on organizationally derived risk drivers that align with business objectives. Security and business continuity management must collaborate to ensure the organization achieves an effective level of operational resiliency at the most efficient cost.

What is the connection to operational risk management?

Operational risk is the risk that emanates from day-to-day operations. It is an unpleasant reality inherent in the activities the organization performs to meet its mission. Operational resiliency is directly affected by how well the organization manages operational risk, which is the fundamental focus of security and business continuity activities. Thus, operational resiliency comes about when security and business continuity are successful in helping the organization to manage operational risk. As a result, many aspects of operational risk management can be found throughout our approach to resiliency engineering.

What is the Resiliency Engineering Framework?

In short, the Resiliency Engineering Framework is the foundation for a process improvement approach to security and business continuity management. It is a framework of practice that integrates security and business continuity activities by defining the essential organizational processes, related goals, and specific practices that are necessary to manage operational resiliency. An organization can use the framework to establish its current level of competency in managing resiliency, set forward-looking resiliency goals and targets, and develop plans to close identified gaps. Bottom line: by taking a process view, the Resiliency Engineering Framework can help an organization to begin building in resiliency and managing it rather than reacting to ever-changing risk environments.

What does it mean to take a "process view" of resiliency?

The success of security and business continuity practices can be short-lived and difficult to measure. Many organizations simply do not know if the practices in which they are investing constrained human and financial resources bring about the results they need to support business objectives. A process view of resiliency puts practices in their appropriate context as part of a larger process. A process, in turn, can be defined, communicated, measured, and controlled; the desired outcomes of the process can be identified, success in reaching these outcomes can be measured, and gaps can be identified and addressed. A process view moves the organization toward longer term, continuous management of resiliency, instead of a reacting to its environment with short-term, unverifiable successes. As a result, the organization can more positively affirm the competency of its security and business continuity programs and approaches rather than describing success in terms of *what hasn't happened*.

Why not build a framework for security or business continuity?

Operational resiliency is dependent on more than just good security and business continuity management. It requires excellence in IT operations and service delivery management and relies on core capabilities that support the organization's ability to achieve its business objectives. For example, enterprise-level activities such as governance, risk management, financial management, and organizational training are all significant contributors to improving and sustaining resiliency. A framework focused on security or business continuity alone would be limiting because these activities alone do not ensure resiliency; only when they are part of a larger enterprise-wide effort do they focus on and support organizational drivers. In addition, building separate frameworks would engender the failure to share requirements, drive toward common goals, and reduce redundancy and cost in the effort to boost operational resiliency. In other words, separate frameworks would solidify the silo-like nature of these activities as they exist in most organizations today.

How is the framework being developed?

The CERT® Resiliency Engineering Framework is being developed by Carnegie Mellon® University's Software Engineering Institute (SEI℠). The project is being led by the Survivable Enterprise Management team of the Networked Systems Survivability program at the SEI. The NSS program is the home of the CERT® Coordination Center. The SEI also is the home to Capability Maturity Model Integration (CMMI), a process improvement model for the development and acquisition of systems and software. The SEI's experience in information security and process improvement provides a unique vantage point from which the lessons of process improvement in the software and systems engineering disciplines can strongly influence similar improvements in the security and business continuity fields. The project also has had the benefit of input from experienced security and business continuity professionals through our collaboration with the Financial Services Technology Consortium (FSTC). FSTC is a forum for collaboration on business and technical issues that affect financial institutions. Because of the nature of their role in sustaining U.S. and world economies, financial institutions have some of the most mature resiliency practices, and have provided a wealth of real-world experience and information to influence the development of the framework. More information about FSTC and its member organizations can be found at www.fstc.org. A list of organizations that have participated in this effort can be found at the end of this document.

Why is the SEI developing this framework?

The SEI has a long history of experience in helping organizations to improve their security and business continuity efforts. We have developed and

® Carnegie Mellon is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.
℠ SEI is a service mark of Carnegie Mellon University.
® CERT is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

transitioned tools, techniques, and methods that organizations use to improve their skill sets and overall capabilities. However, we recognize that technological innovation and improved skill sets alone have not resulted in measurable improvements in security or business continuity for many organizations. What is often missing is an active management component focused on outcomes and aligned with business drivers. In the Resiliency Engineering Framework, the vital linkages between security, business continuity, IT operations management, and other core competencies are captured in the process definition, and the emphasis is on managing these competencies to the best possible outcome for the organization. Future benefits of such a framework include the ability to benchmark organizational performance in managing resiliency. In addition, the framework may help organizations to ease their compliance burdens by establishing a sustained level of competency that can be independently verified.

Who would use the framework and how?

Security and business continuity professionals will use the Resiliency Engineering Framework to improve their respective efforts. However, the framework is intended to be applied enterprise-wide because it encompasses the skills and competencies of a wide range of organizational functions. Thus, implementation of the framework requires organizational sponsorship and needs to be directed at a sufficiently high level in the organization where resources can be commanded across departmental and organizational unit lines. Ideally, a chief risk manager or other senior-level executive (such as a CIO or CSO) would sponsor and direct a resiliency process improvement effort. Auditors and chief audit executives will also find the framework useful as a basis for evaluating their organization’s capability to manage operational risk.

What is covered by the framework?

The Resiliency Engineering Framework covers security and sustainability processes across four broad categories: engineering, enterprise management, operations management, and process management. It focuses on business-critical services, their related business processes, and the assets that are used by these services and processes to meet their missions: people, information, technology, and facilities. The emphasis is on developing, implementing, and managing protection and sustainability strategies for these assets in alignment with their importance to the business processes they support and the business objectives they help the organization to achieve. In addition, the framework includes many enterprise-level processes that contribute to resiliency but are often not explicitly considered. While the framework focuses on the interdependencies and collaboration between similarly-focused risk activities like security and business continuity, it also addresses the contributions of effective IT operations and service delivery management—an area that shares organizational responsibility for a strong and viable control structure. To date, twenty-four distinct processes that are essential to managing resiliency have been identified and codified.

How does the framework differ from existing best practices models?

The Resiliency Engineering Framework should not be viewed as a competitor to or a replacement for existing best practices in the fields of security, business continuity, or IT service management. Instead, it helps an organization to make better use of these practices by providing a process definition into which these practices fit and are executed in the pursuit of process goals. In other words, by emphasizing process definition, management, measurement, and improvement, an organization can use any combination of best practices to fulfill the process goals. In this way, an organization that employs more than one framework can make efficient and effective use of them by relating them to the higher order process goals of the Resiliency Engineering Framework.

What are some of the additional benefits of the framework?

The Resiliency Engineering Framework helps organizations to take a systematic and structured approach to managing security, business continuity, and operational resiliency in context with business objectives. Thus, the organization expands its capabilities to actively manage to resiliency goals rather than being relegated to ad hoc, reactive, fire-fighting, and hero-based approaches. In essence, the process becomes the foundation for the activities and practices that are carried out on a day-to-day basis in the security department, in business continuity planning, and in managing IT operations. In addition, as the framework matures, organizations may be able to use it to benchmark their capabilities against other organizations in their industry. They may even be able to apply the framework to their business partners to validate their commitment to resiliency management and to ensure end-to-end resiliency of critical business processes. An industry benchmark can also help organizations to comply with current relevant regulations and to influence the need for future regulations by reflecting the current state of best practices.

Can the framework be used with other process improvement efforts?

The Resiliency Engineering Framework was designed to be open and extensible. Thus, organizations that have experience with model-based process improvement should be able to adopt and assimilate the Resiliency Engineering Framework into their existing efforts. Because of its design and presentation, any process improvement technique used by an organization should be able to be extended to the framework.

Is there an assessment methodology for the framework?

Concurrent with the development of the framework, an initial set of surveys is being developed that can help an organization to determine its current level of competency for managing resiliency. These surveys are not meant to appraise process maturity or capability, but instead to give the organization a way to begin its process improvement efforts by determining its current level of practice. In the future, there are plans to offer an official appraisal methodology that will allow organizations to measure their capability for managing resiliency as an enterprise process.

Is there training available?

At present, there is no official training course focused on the concepts of resiliency engineering or management. However, as the framework is introduced to the community and more experience is gained in using it in a process improvement environment, training will be developed and offered. In addition, we have been expanding our instruction in the OCTAVE® methodology to include discussion of the movement of security toward resiliency. The SEI offers a schedule of OCTAVE courses throughout the year, which can be viewed at http://www.sei.cmu.edu/products/courses/courses.html#SEC.

How can my organization begin to use the framework?

® OCTAVE is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. OCTAVE is the Operationally Critical Threat, Asset, and Vulnerability Evaluation. More information on this methodology can be found at http://www.cert.org/octave.

An initial draft of the framework with initial guidelines for process improvement will be released in the April 2007 time frame as an SEI-published technical report. An organization may use the information in this technical report to begin process improvement and implementation of the framework. In the near future, the SEI also will make available a limited number of assessment, pilot, and research collaboration opportunities related to further development of this model in which your organization can become involved.

How can my organization get involved in this project?

Beginning in February 2007, you can join our effort in any of these four ways:

- participating in an SEI-led evaluation of your current resiliency practices
- participating in a process improvement pilot using the framework
- becoming an SEI research collaboration partner to further develop the model
- joining the REF user's group that is beginning to form

In addition, the SEI will also entertain customer-specific collaborative engagements that may involve a customized combination of more than one of these offerings. More about these opportunities will be released by the SEI in the next few months.

What are the benefits of involvement in this project?

Organizations that collaborate with the SEI on the continuing research and development of the Resiliency Engineering Framework will benefit from early access and use of project and framework artifacts and will have an opportunity to influence the ongoing research and development. In addition, collaborators will enjoy direct benefits from deploying the resiliency engineering concepts in their operations. For organizations that provide services in security or business continuity, early access to REF artifacts will allow them to be positioned to provide services based on the framework once it is released; these organizations also may qualify to lead controlled pilots at selected customer sites prior to the release of the framework.

Who are the points of contact?

To become involved in the Resiliency Engineering Framework project, you may contact Joe McLeod at jmcleod@sei.cmu.edu. Current documents that describe the framework and underlying concepts can be found at http://www.cert.org/nav/index_green.html under the title "ESM."