HISTORY OF CERT-RMM

February 2013

The establishment of the CERT Resilience Management Model actually began during the development and deployment of the OCTAVE methodology, which was focused on improving an organization's involvement in managing information security risks. Through this work, we realized that organizations often view security as a technical specialty and don't usually associate it with other activities such as business continuity and IT operations management—all of which are focused on managing operational risk and sustaining operational resilience. Absent this important business driver, it is difficult to position security (or business continuity planning) as an enabler of an organization's strategy, much less an activity that is worthy of the investment of limited resources such as capital and people.

By examining the impact of OCTAVE and relying on the CERT Division's vast expertise in the field of security, we began to envision ways that the convergence of security, business continuity, and IT operations management could become an important contributor to an organization's success and growth. Combined with the Software Engineering Institute's successful history of developing and deploying process improvement models for software and systems engineering, we realized that a process improvement approach to managing operational resilience could help organizations to raise the effectiveness of their current efforts by shifting their perspective to the process, not the practice.

Along the way, we have supplemented our research by seeking out real-world problems to solve. In 2004, we began a partnership with the Financial Services Technology Consortium (FSTC), now the BITS Financial Roundtable (http://www.bits.org/), to examine the application of these concepts to the complex problem of managing operational resilience in the U.S. financial sector. This has given us unparalleled access to some of the best practitioners in the security and business continuity space.

Through our collaboration with the FSTC, as well as from extensive review of existing codes of practice in the areas of security, business continuity, and IT operations management, the CERT Division codified a draft process definition for operational resilience management processes called the Resiliency Engineering Framework (REF). The framework described the range of processes that characterize the organizational capabilities necessary to actively direct, control, and manage operational resilience. FSTC organizations began benchmarking their performance against the framework to characterize industry performance, validate the framework, and begin process improvement efforts. Along with this benchmarking activity, the CERT Division began developing an appraisal method.

The last version of the REF, V0.95R, was released in April 2008 for comment and review. It is still available for download for reference purposes.

In 2009, release of an expanded, revised version of the framework began under a new name, the CERT Resilience Management Model. In 2010, the initial version of CERT-RMM, V1.0 was released to the community. An updated version of this model with supporting adoption and use information, CERT-RMM V1.1, was published as an Addison-Wesley publication.

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

[no markings required]

DM18-0213