MEASURES FOR MANAGING OPERATIONAL RESILIENCE

JULIA ALLEN

The SEI\(^1\) has devoted extensive time and effort to defining meaningful metrics and measures for software quality, software security, information security, and continuity of operations. The ability of organizations to measure and track the impact of changes—as well as changes in trends over time—are important tools to effectively manage operational resilience, which is the measure of an organization’s ability to perform its mission in the presence of operational stress and disruption. For any organization—whether Department of Defense (DoD), federal civilian agencies, or industry—the ability to protect and sustain essential assets and services is critical and can help ensure a return to normalcy when the disruption or stress is eliminated. This article describes our research to help organizational leaders manage critical services in the presence of disruption by presenting objectives and strategic measures for operational resilience, as well as tools to help them select and define those measures.

In April 2011, the DoD identified\(^2\) the engineering of resilient systems as a top strategic priority in helping to protect against the malicious compromise of weapons systems and to develop agile manufacturing for trusted and assured defense systems. SEI CERT has been exploring the topic of managing operational resilience at the organizational level for the past seven years through development and use of the CERT Resilience Management Model (CERT-RMM)\(^3\), a capability model designed to establish the convergence of operational risk and resilience management activities and apply a capability level scale that expresses increasing levels of process performance. CERT-RMM measures the ability of an organization to protect and sustain high-value services (which are organizational activities carried out in the performance of a duty or production of a product) and high-value assets (which are items of value to the organization, such as people, information, technology, and facilities that high-value services rely on). Resilient systems, as identified by the DoD, is one category of technology asset.

Reprinted with permission.
Our research on resilience measurement and analysis focuses on addressing the following questions, which are often asked by organizational leaders:

1. How resilient is my organization?
2. Have our processes made us more resilient?
3. What should be measured to determine if performance objectives for operational resilience are being achieved?

To establish a basis for measuring operational resilience, we relied on the CERT-RMM as the process-based framework against which to measure. CERT-RMM comprises 26 process areas (such as Incident Management and Control (IMC) and Asset Definition and Management (ADM)) that provide a framework of goals and practices at four increasing levels of capability (Incomplete, Performed, Managed, and Defined.)

Our initial work provided organizational leaders with tools to determine and express their desired level of operational resilience. Specifically, we defined high-level objectives for an operational resilience management program, for example, “in the face of realized risk, the program ensures the continuity of essential operations of high-value services and their associated assets.” We then demonstrated how to derive meaningful measures from those objectives using a condensed Goal Question (Indicator) Metric method (refer to Park 1998), for example, determining the probability of delivering service through a disruptive event. We also defined a template for defining resilience measures and presented example measures using the template.

Too often, organizations collect “type count” measurements (such as numbers of incidents, systems with patches installed, or people trained) with little meaningful context on how these measures can help inform decisions and affect behavior. Based on the Goal Question (Indicator) Metric method, we identified strategic measures that help organizational leaders determine which process-level measures best address their needs. What follows is a description of five organizational objectives for managing operational resilience and 10 strategic measures for an operational resilience management (ORM) program. The ORM program defines an organization’s strategic resilience objectives (such as ensuring continuity of critical services in the presence of a disruptive event) and resilience activities (such as the development and testing of service
continuity plans). We use an example of acquiring managed security services from an external provider to show how each measure could be used. Managed security services may include network boundary protection (such as firewalls and intrusion detection systems), security monitoring, incident management (such as forensic analysis and response), vulnerability assessment, penetration testing, and content monitoring and filtering.

**Organizational objective 1:** The ORM program derives its authority from—and directly traces it to—organizational drivers (which are strategic business objectives and critical success factors), as indicated by the following measures:

- **Measure 1:** Percentage of resilience activities that do not directly (or indirectly) support one or more organizational drivers.
  
  **Example use:** External security services replace comparable in-house services with a lower cost (less effort) and more effective (less impact from incidents) solution. After external security services are operational, 75 percent of in-house efforts no longer support organizational drivers. This measure can be used to ensure an effective transition of designated in-house services to externally-provided services and to retrain/reassign staff currently performing such services.

- **Measure 2:** For each resilience activity, the number of organizational drivers that require it to be satisfied (the goal is equal to or greater than 1).
  
  **Example use:** An example of a resilience activity is formalizing a relationship with a security services provider using a contract or service level agreement (SLA) that includes all resilience specifications. There is at least one organizational driver that calls for having security services in place to achieve the driver. This driver likely maps to a personal objective of the chief information officer or chief security officer. If there is no such traceability, one or more drivers may require updating.

**Organizational objective 2:** The ORM program satisfies resilience requirements that are assigned to high-value services and their associated assets, as indicated by the following measures:

- **Measure 3:** Percentage of high-value services that do not satisfy their assigned resilience requirements.
  
  **Example use:** Resilience requirements for security services are specified in the SLA. Provider performance is periodically reviewed to ensure that all services are meeting the SLA requirements (for example, high priority alerts from incident detection systems are resolved within xx minutes). Optimally, this percentage should be zero. If it is greater than an SLA-stated threshold (for example, 20 percent for service A), corrective action is taken and confirmed.

- **Measure 4:** Percentage of high-value assets that do not satisfy their assigned resilience requirements.
  
  **Example use:** This example is similar to the one above. The incident database is a high-value asset that is required to provide incident response services. The SLA specifies resilience requirements for
this database, including daily automated backups and quarterly and event-driven (backup server upgrade and high-impact security incident) testing to ensure the provider’s ability to successfully restore from backups. Optimally, this percentage should be zero. If it is greater than an SLA-stated threshold (for example, 20 percent for asset B), corrective action is taken and confirmed.

Organizational objective 5: The ORM program—via the internal control system—ensures that controls for protecting and maintaining high-value services and their associated assets operate as intended, as indicated by the following measures:

- **Measure 5**: Percentage of high-value services with controls that are ineffective or inadequate.

  **Example use**: The SLA identifies the controls (policies, procedures, standards, guidelines, tools, etc.) that are required by a service. These controls can be tailored versions of the controls that the organization uses or can be negotiated based on the provider’s standard suite of controls. Provider implementation of these controls is periodically reviewed (audited, assessed, scans performed, etc.). Optimally, this percentage should be zero. If it is greater than an SLA-stated threshold (for example, 20 percent for service A), corrective action is taken and confirmed.

- **Measure 6**: Percentage of high-value assets with controls that are ineffective or inadequate.

  **Example use**: This measure is as described above, with asset controls stated in the provider SLA.

Organizational objective 4: The ORM program manages operational risks to high-value assets that could adversely affect the operation and delivery of high-value services, as indicated by the following measures:

- **Measure 7**: Confidence factor that risks from all sources that require identification have been identified.

  **Example use**: Major sources of risk are initially identified in the provider SLA and as part of an ongoing review based on changes in the operational environment within which services are provided. The elements that contribute to “confidence factor” (such as risk thresholds by service) are also identified. Confidence factor is represented as a Kiviat diagram showing plan versus actual for all sources. Analysis of provider gaps is reviewed on a periodic basis and corrective action is taken and confirmed to reduce unacceptable gaps.

- **Measure 8**: Percentage of risks with impact above threshold.

  **Example use**: Assessment of provider risk is performed on a periodic basis as specified in the SLA. Optimally, this percentage should be zero. If it is greater than an SLA-stated threshold (for example, 20 percent for risk type A), corrective action is taken and confirmed.

Organizational objective 5: The ORM program ensures the continuity of essential operations of high-value services and their associated assets in the face of realized risk, as indicated by the following measures:
• **Measure 9:** Probability of delivered service through a disruptive event.

**Example use:** The SLA states service-specific availability and service levels to meet, both steady state and in degraded mode. Provider performance is periodically reviewed, including during and after a disruptive event (power outage, cyber attack, etc.). Probability of delivered service is determined and evaluated as a trend over time. Corrective action is taken and confirmed as required.

• **Measure 10:** For disrupted, high-value services with a service continuity plan, percentage of services that did not deliver service as intended throughout the disruptive event.

**Example use:** The SLA includes requirements for service-specific continuity (SC) plans. For provider services with SC plans that do not maintain required service availability and service levels, corrective actions are taken and confirmed, including updates to SC plans. In addition, the customer uses this as an opportunity to review and update its own SC plans that depend on provider services, where service was not delivered as intended.

All these strategic measures derive from lower-level measures at the CERT-RMM process area level, including average incident cost by root cause type and number of breaches of confidentiality and privacy of customer information assets resulting from violations of provider access control policies.

To help organizational leaders determine what measures work best for their organization, we are collaborating with members of the CERT-RMM Users Group, which includes the United States Postal Inspection Service, Discover Financial Services, Lockheed Martin, and Carnegie Mellon University. Through a series of two-day workshops, members define an improvement objective, assess their current level of operational resilience against that objective, identify areas of improvement, and implement improvement plans using the CERT-RMM processes and candidate measures as the guide. Please contact us if you are interested in joining a CERT-RMM Users Group.

**ADDITIONAL RESOURCES**

To learn more about CERT work in Resilience Measurement, please visit http://www.cert.org/resilience/rma.html

- To read the SEI technical note, *Measuring Operational Resilience Using the CERT Resilience Management Model*, please visit www.sei.cmu.edu/reports/10tn030.pdf
- To read the SEI technical report, *Measures for Managing Operational Resilience*, please visit www.sei.cmu.edu/library/abstracts/reports/11tr019.cfm
- To listen to a podcast that describes CERT work in Resilience Measurement, please visit www.cert.org/podcast/show/20111004allen.html

For more information about the CERT Resilience Management Model (CERT-RMM), please visit www.cert.org/resilience/rmm.html

© Copyright 2011 Carnegie Mellon University
To read an article about how the CERT Resilience Management Model helps companies predict performance under stress, please visit page 8 of the SEI 25th Anniversary Year in Review, www.sei.cmu.edu/library/assets/annualreports/2010_Year_in_Review.pdf

Notes

1. http://www.sei.cmu.edu/measurement/index.cfm
2. http://www.acq.osd.mil/ddre/publications/docs/OSD_02073_11.pdf
3. http://www.cert.org/resilience/rmm.html
4. http://www.sei.cmu.edu/library/abstracts/reports/10tn030.cfm
5. http://www.sei.cmu.edu/reports/96hb002.pdf
6. http://en.wikipedia.org/wiki/Radar_chart
7. http://www.sei.cmu.edu/library/abstracts/reports/11tr019.cfm
8. http://www.sei.cmu.edu/training/p92.cfm

Julia Allen is a principal researcher within the CERT® Program at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University in Pittsburgh, PA. Allen’s areas of interest include operational resilience, software security and assurance, and measurement and analysis.

Prior to this technical assignment, Allen served as acting Director of the SEI for an interim period of 6 months as well as Deputy Director/Chief Operating Officer for 3 years. Prior to joining the SEI in 1992, she was a vice president in embedded systems software development for Science Applications International Corporation and managed large software development programs for TRW (now Northrop Grumman). Her degrees include a B.Sci. in Computer Science (University of Michigan) and an MS in Electrical Engineering (University of Southern California).

Allen is the author of The CERT Guide to System and Network Security Practices (Addison-Wesley 2001) and moderator for the CERT Podcast Series: Security for Business Leaders. She is a co-author of Software Security Engineering: A Guide for Project Managers (Addison-Wesley 2008) and CERT Resilience Management Model (RMM): A Maturity Model for Managing Operational Resilience (Addison-Wesley 2011).

ANY CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT. © CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.