Risk and Resilience: Considerations for Information Security Risk Assessment and Management

Julia Allen and Jim Cebula
CERT Program
Software Engineering Institute

Session ID: GRC-202
Session Classification: Intermediate
Objectives

- Get you talking a common language about risk concepts
- Introduce you to the CERT Resilience Management Model
- Start you thinking about these concepts in your organization
Some Questions to Consider

- Performance or compliance measures?
- Are you measuring at all?
- Reactive or proactive?
- Can you sustain your performance under stress? How would you know?
- Do you have a process to manage your monitoring efforts?
- What is your organization’s risk tolerance?
- Who is responsible for accepting risk? Is there a process?
- What risks has the organization accepted?
Words Matter...

Vulnerability  Exposure

Condition

Risk

Threat  Consequence

Impact  Weakness
Elements of Risk
The Basic Risk Equation

RISK = CONDITION + CONSEQUENCE
Assembling the Risk Elements

RISK

WEAKNESS OR EXPOSURE

ACTOR
MOTIVE
OUTCOME
Assembling the Risk Elements

RISK

WEAKNESS OR EXPOSURE

THREAT

ACTOR

MOTIVE

OUTCOME

CONDITION of RISK
Positioning “Impact” in Risk

CONSEQUENCE of RISK
Outcome vs. Consequences

**Outcome** - unwanted or unintended results of an actor with a motive exploiting a weakness, exposure, or vulnerability

Examples:
- Access to email or critical systems is denied
- Network is slow; users can’t access Internet
- Customers can’t place orders on web site
- Remote sensors shut down on gas valves causing explosion

**Consequence** refers to the impact on a person or organization as a result of the exploitation

Examples:
- Loss of $50,000 in revenue per hour
- Productivity loss of 45% resulting in $500,000 of rework
- Reputational damage due to news coverage
- Fine of $1,000,000
- Loss of life for 20 employees
Adding Uncertainty

RISK
WEAKNESS OR EXPOSURE
ACTOR MOTIVE OUTCOME IMPACT
CONDITION CONSEQUENCE

How frequent or probable is this threat scenario

RSA 2011 CONFERENCE
CERT | Software Engineering Institute Carnegie Mellon
It All Adds Up To …
Operational Risk
Basic Types of Risk

- Four generally accepted types of risk:
  1. Hazard
  2. Financial
  3. Operational
  4. Strategic

- Boundaries can overlap—for example:
  - Hazard risk (fire, flood) can be a component of operational risk.
  - Strategic risk can include financial risks related to strategy decisions.
Operational Risk

- A form of hazard risk affecting day-to-day business operations
- The potential failure to achieve mission objectives
- Inclusive of “security risks”
Operational Risk Management
Operational Risk Management

A continuous cycle of operational risk management activities
Risk Avoidance vs. Risk Mitigation

Reduce likelihood of threat and/or...

Reduce effects on organization

RISK

THREAT

ACTOR MOTIVE OUTCOME IMPACT

CONDITION CONSEQUENCE

Software Engineering Institute Carnegie Mellon

CERT
Risk Monitoring and Control

- Process of
  - identifying, analyzing, and planning for new risks
  - monitoring existing risks and their response strategies (for effectiveness)
  - monitoring the status of residual risks
  - identifying and implementing triggers to determine when risks should be reviewed, new risk identification should occur, etc.

- Once a risk response has been implemented, risks do not go away!
Where Does Risk Assessment Fit?

- Risk assessment includes:
  - Risk planning
  - Risk identification
  - Risk analysis
  - Risk response
- It is the “diagnostic” part of the continuous risk management cycle
Vulnerability vs. Risk Assessment

- **Vulnerability assessment** is a means to identify threats: weaknesses, exposures, and vulnerabilities
  - Examples:
    - Running automated assessment tools
    - Doing penetration tests

- **Risk assessment** is a process of identifying risks relative to threat; includes probability, impact, and consequence

Vulnerability assessment is NOT equal to risk assessment.
Risk and Resilience
Resilience Defined

- The physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit
  [wordnet.princeton.edu]

Parsed in organizational (and operational) terms:

_The emergent property of an organization that can continue to carry out its mission after disruption that does not exceed its operational limit_

Where does the _disruption_ come from? Realized risk.
Operational Risk and Operational Resilience

- Known risk is addressed before it becomes disruptive.
- Organizations can more easily predict the performance of business services under uncertain conditions (i.e., unknown risks).

An operationally-resilient service

- Can meet its mission under adverse circumstances (times of stress, within some limit)
- **AND** return to normal when the adversity (stress) is eliminated
Convergence directly affects the level of operational resilience.

Level of operational resilience affects the ability to meet organizational mission.
Protection, Sustainability, and Risk

Basic risk equation

Protection & sustainability

- **Protect**: Manage *Conditions* of Risk
- **Sustain**: Manage *Consequences* of Risk
The CERT Resilience Management Model (CERT-RMM)
What is CERT-RMM?

- CERT-RMM is a maturity model for managing and improving operational resilience.

  - Guides implementation and management of operational resilience activities
  - Converges key operational risk management activities: security, BC/DR, and IT operations
  - Defines maturity through capability levels (like CMMI)
  - Improves confidence in how an organization responds in times of operational stress
Layers of Resilience Activities

Resilience planning, program execution, and coordination across organizational units

Operational Resilience Management System

Security and Control Activities
Developing and implementing security architectures, managing security operations

IT Operations Activities
Developing, implementing, and managing processes to deliver IT services and manage IT infrastructures

Continuity and Recovery Activities
Developing and executing continuity plans, recovery plans, and restoration plans

Tactical execution of resilience activities
Imperatives for Building CERT-RMM

- Increasingly complex operational environments where traditional approaches are failing
- Siloed nature of operational risk activities; a lack of convergence
- Lack of common language or taxonomy
- Overreliance on technical approaches
- Lack of means to measure managerial competency
- Inability to confidently predict outcomes, behaviors, and performance under times of stress
CERT-RMM Background

- Collaboration with high maturity organizations
- 20+ years of security mgmt knowledge at CERT
- CMMI architecture and experience
- 800+ practices for security, BC, & IT ops
- Piloting in private and government organizations
Organizational Context

Service Mission

Business Processes

Assets in Production

Operational Resilience Management Processes

CERT-RMM focuses here
# CERT-RMM: 26 Process Areas in 4 Categories

<table>
<thead>
<tr>
<th>Engineering</th>
<th>Operations Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM Asset Definition and Management</td>
<td>AM Access Management</td>
</tr>
<tr>
<td>CTRL Controls Management</td>
<td>EC Environmental Control</td>
</tr>
<tr>
<td>RRD Resilience Requirements Development</td>
<td>EXD External Dependencies</td>
</tr>
<tr>
<td>RRM Resilience Requirements Management</td>
<td>ID Identity Management</td>
</tr>
<tr>
<td>RTSE Resilient Technical Solution Engineering</td>
<td>IMC Incident Management &amp; Control</td>
</tr>
<tr>
<td>SC Service Continuity</td>
<td>KIM Knowledge &amp; Information Management</td>
</tr>
<tr>
<td></td>
<td>PM People Management</td>
</tr>
<tr>
<td></td>
<td>TM Technology Management</td>
</tr>
<tr>
<td></td>
<td>VAR Vulnerability Analysis &amp; Resolution</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Management</td>
<td>Process Management</td>
</tr>
<tr>
<td>COMM Communications</td>
<td>MA Measurement and Analysis</td>
</tr>
<tr>
<td>COMP Compliance</td>
<td>MON Monitoring</td>
</tr>
<tr>
<td>EF Enterprise Focus</td>
<td>OPD Organizational Process Definition</td>
</tr>
<tr>
<td>FRM Financial Resource Management</td>
<td>OPF Organizational Process Focus</td>
</tr>
<tr>
<td>HRM Human Resource Management</td>
<td></td>
</tr>
<tr>
<td>OTA Organizational Training &amp; Awareness</td>
<td></td>
</tr>
<tr>
<td>RISK Risk Management</td>
<td></td>
</tr>
</tbody>
</table>

**Certification logos:**

![CERT logo](CERT.jpg)

![RSA Conference logo](RSA2011.jpg)

**Software Engineering Institute logo:**

![Software Engineering Institute logo](SEI.jpg)
Process Institutionalization in CERT-RMM

Practices are performed

Processes are acculturated, defined, measured, and governed

Level 3
• Defined

Level 2
• Managed

Level 1
• Performed

Level 0
• Incomplete

Higher degrees of institutionalization translate to more stable processes that
• produce consistent results over time
• are retained during times of stress
A Risk “Ecosystem” in CERT-RMM

Continuous risk management process defined and executed

[Diagram showing relationships between different components of risk management process]
Summary

- We’ve given you a common, structured way to discuss
  - Elements of Risk
    - Condition
    - Consequence
    - Uncertainty
  - Operational Risks
  - Continuous Risk Management
  - Vulnerability Assessment
  - Resilience
- We’ve also introduced CERT-RMM, which can help you
  - Improve processes
  - Bring together IT Ops, Security, and BC/DR
Apply - Things To Do Next Week

- Start a conversation (IT, Security, and BC/DR should all be working together)
- Try to answer any two of our opening “questions to consider” in your organization.
- Choose one RMM process area and start working through the specific practices.
Questions?
Julia Allen  
RMM Developer/Measurement Team Lead  
jha@sei.cmu.edu

Jim Cebula  
Information Resilience Team Lead  
jcebula@cert.org

David White  
RMM Transition Lead & Developer  
dwhite@cert.org

Lisa Young  
RMM Appraisal Lead & Developer  
lry@cert.org

Rich Caralli  
Technical Manager,  
Resilient Enterprise Management  
rcaralli@cert.org

SEI Customer Relations  
customer-relations@sei.cmu.edu  
412-268-5800

Joe McLeod  
For info on working with us  
jmcleod@sei.cmu.edu

Richard Lynch  
Public Relations — All Media Inquiries  
public-relations@sei.cmu.edu
NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE 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.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.