Advanced Risk Analysis for High-Performing Organizations

Christopher Alberts
Audrey Dorofee

Sponsored by the U.S. Department of Defense
© 2006 by Carnegie Mellon University
**Report Documentation Page**

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

<table>
<thead>
<tr>
<th>1. REPORT DATE</th>
<th>2. REPORT TYPE</th>
<th>3. DATES COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td></td>
<td>00-00-2006 to 00-00-2006</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
<th>5a. CONTRACT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Risk Analysis for High-Performing Organizations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carnegie Mellon University, Software Engineering Institute, 5000 Forbes Avenue, Pittsburgh, PA, 15213-3890</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>10. SPONSOR/MONITOR’S ACRONYM(S)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>11. SPONSOR/MONITOR’S REPORT NUMBER(S)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>12. DISTRIBUTION/AVAILABILITY STATEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release; distribution unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13. SUPPLEMENTARY NOTES</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>14. ABSTRACT</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>15. SUBJECT TERMS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>16. SECURITY CLASSIFICATION OF:</th>
<th>17. LIMITATION OF ABSTRACT</th>
<th>18. NUMBER OF PAGES</th>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. REPORT</td>
<td>b. ABSTRACT</td>
<td>c. THIS PAGE</td>
<td>Same as Report (SAR)</td>
</tr>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
<td></td>
</tr>
</tbody>
</table>

Standard Form 298 (Rev. 8-98) 
Prepared by ANSI Z39-18
# Changing Operational Environment

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized management control of processes</td>
<td>Distributed management control of processes</td>
</tr>
<tr>
<td>Dedicated, stand-alone technologies</td>
<td>Interoperable, networked technologies</td>
</tr>
<tr>
<td>Permanent enterprise, defined by organizational chart</td>
<td>Virtual enterprise, defined by mission</td>
</tr>
<tr>
<td>One team, one mission</td>
<td>Many teams, one mission</td>
</tr>
<tr>
<td>Compartmentalized view of risk (e.g., project, security)</td>
<td>Integrated view of risk</td>
</tr>
</tbody>
</table>
Changing Risk Profiles

Changes in operational environments are driving the need for advanced risk analysis techniques.

• The operational environment is becoming more complex (e.g., distributed processes).

• New types of risks have emerged from this complexity.
  - inherited risk
  - new sources of risk (e.g., cyber-security risks)
  - risk from combinatorial effects
  - risk from cascading consequences
  - risk from emergent threats
The Need for Advanced Techniques

High-performing organizations are able to manage traditional risks.

Risks arising from operational complexity are often subtle in nature, but bring the potential for catastrophic consequences.

High-performing organizations have the basic skills needed to manage these new types of risk, but sufficient techniques are not readily available.
Key Requirements

High performers need advanced risk management techniques that enable them to

• assume an integrated view of risk (one view that includes process, technology, security, and interoperability risks)

• address the interrelated nature of risk (combinatorial effects and cascading consequences)

• understand the amount of risk that is inherited from partners and collaborators

• characterize the risk arising from the emergent properties of a distributed process
What Is Risk?

The possibility of suffering harm or loss

Risk requires the following conditions:
• loss
• uncertainty
• choice
Nature of Risk

Speculative (dynamic) – a risk that has profit and loss associated with it

Hazard (static) – a risk that only has loss associated with it
Operational Risk

The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events

A broad range of threats must be considered when analyzing the potential for mission success.
A mission threat is a fundamental flaw, or weaknesses, in the purpose and scope of a work process.
A design threat is an inherent weakness in the layout of a work process.
An activity threat is a flaw, or weaknesses, arising from the manner in which activities are managed and performed.
An environment threat is an inherent constraint, weakness, or flaw in the overarching operational environment in which a process is conducted.
An event threat is a set of circumstances triggered by an unpredictable occurrence that introduces unexpected change into a process.
Mission Risk

The possibility that a mission might not be successfully achieved
Mission Assurance

Establishing a reasonable degree of confidence in mission success

Mission assurance is achieved by ensuring that risk to the mission (i.e., mission risk) is within tolerance.

A key aspect of mission assurance is its dual focus on outcome and execution.
Mission Assurance Strategy

Reduce mission risk to an acceptable level

- process design and management techniques

- risk management techniques

Resolve problems that occur

- problem management techniques
What is MAAP?

MAAP is a protocol, or heuristic, for determining the mission assurance of an operational process or system.
Key Characteristics of MAAP

Applies an engineering approach to risk analysis

Designed for highly complex environments (multi-organization, system of systems)

Provides an in-depth analysis of processes, relationships, and dependencies

Characterizes the risk of mission failures
  • process performance risk
  • security risk
  • operational environment risk
Structured Analysis of Performance

MAAP analyzes process performance in multiple operational states
- normal, or expected, operational conditions
- unusual circumstances, or occurrences, triggered by external events
Analyzing Multiple States

State 1: Expected Operational Conditions

State 2: When Stressed by Event 1

State 3: When Stressed by Event 2

Risk resulting from event 1

Risk resulting from event 2

Risk during expected operational conditions

Risk to the mission
Risk Causal Chain

Risk during expected operational conditions

Risk from event 1

Risk from event 2

Risk resulting from different operational circumstances

Combinations of threats, vulnerabilities and controls

Mission risk

© 2006 by Carnegie Mellon University
Bringing Risk within Tolerance

There is a significant gap between actual risk exposure and management’s goal.

Risk tolerance

© 2006 by Carnegie Mellon University
Key Risk Drivers

A critical path analysis identifies the key risk drivers.
Protocol Fundamentals - 1

• Determine mission objectives.

• Characterize all operations conducted in pursuit of the mission.

• Define risk evaluation criteria in relation to the mission objectives.

• Identify potential failure modes.

• Perform a root cause analysis for each failure mode.
Protocol Fundamentals - 2

• Develop a risk profile of the mission.

• Ensure that mission risk is within tolerance.
A Common Basis for Analysis

MAAP

Incident Management Model
- Incident Management Analysis

Software Process Model
- Software Process Analysis

Operational Security Model
- Operational Security Analysis

Other Models
- Other Analyses
MAAP Pilot

Analyzed an incident management process in a large government organization

Analyzed risk to the mission under normal conditions
   • quality of response
   • timeliness of response
   • customer satisfaction

Examined risk to the mission under unusual circumstances
   • two major incidents occur at the same time
   • cyber security attack renders ticketing system unavailable for an extended period of time
Example: Process Workflow

Detect, Triage, and Respond to Events

- If escalates to Call Center Tier 2:
  - Monitor queue
  - Receive call

- If escalates to other groups:
  - Monitor events and indicators
  - Resolve and annotate

- If resolved and no action required:
  - If escalated to other groups:
    - Implement actions and close ticket
  - To Field: Implement actions and close ticket

- If escalations to IR Team or Call Center Tier 2:
  - If resolved and no action required:
    - If escalated to other groups:
      - Implement actions and close ticket
  - To Field: Implement actions and close ticket

Note: The workflow is a snapshot, based on available information.
Example: Complex Risks

- Events could be unnecessarily escalated by the Call Center.
- IDS tools inherently provide false positives.
- IDS tools provide false positives.
- Inadequate and inefficient tuning of IDS tools exacerbates false positives.
- False positives could be forwarded by the Watch Office.
- There is limited back-up capability for IDS tuning in IRC.
- There are insufficient tools and templates to support IR Team's tasks.
- It is difficult to find qualified technical staff.
- IR Team is a bottleneck.
- There is inadequate equipment to support Watch Office on-line training.
- There is a lack of a comprehensive and balanced training and cross-training program.
- There is no QA for training.
- The training program is inadequate.
- SOC staff have uneven skills for recognizing false positives.
- False positives could be forwarded by the Watch Office.
- There is limited time and opportunity to stay current in field.
- The training program is inadequate.
- IRC partnership determines who fills what position.
  The best person is not always selected.
- Site's do not always tell CIRC when they are performing internal scans.
- There is a heavy reliance on Pre-existing KSAs.
- There is a heavy reliance on on-the-job training.
- An understaffed mission could lead to problems with response time and quality.
- There is a heavy reliance on Pre-existing KSAs.
- Training is informal and based on mentoring.
- All security events go to IR Team.
- SET assumes responsibility for too many tasks relative to the number of staff.
- Events could be unnecessarily escalated by the Call Center.
Example: Mission Risk

Mission Risk Exposure

- Severe
- High
- Medium
- Low
- Minimal

Current value of mission risk exposure

Time
Example: Mission Assurance Goal

Management’s goal is to build a “world-class” incident management capability.

This goal translates to very high mission assurance (i.e., very low risk to the mission).
Example: Gap in Performance

There is a significant gap between actual performance and management’s goal.
Example: Mitigation Strategy

• Simplify the mission.
  - Determine which incident management services are essential.
  - Develop a plan for growing the incident management capability over time.

• Redesign the process based on the revised mission.

• Develop and test contingency plans.
Conclusions

Many types of risk prevalent in today’s operational environments (e.g., event risks, inherited risk) are not readily identified using traditional risk analysis techniques.

High-performing organizations have the basic skills needed to identify and manage these new types of risk, but lack sufficient techniques.

Average or poor performers will not have the skills needed to identify and manage new types of risk (and probably have bigger, more obvious risks to deal with).

MAAP is one technique that high performers can use to identify and mitigate the risks arising from operational complexity.
Additional Research and Development

Develop a technique for quickly estimating mission risk exposure.
  • First pilot will focus on mission assurance in incident management.
  • Second pilot will focus on mission assurance in system development.

Refine and document MAAP based on pilot experience.

Pilot MAAP in another domain.
Contact Information

Telephone  412 / 268-5800

Fax  412 / 268-5758

WWW  http://www.sei.cmu.edu/programs/acquisition-support/

U.S. mail  Customer Relations
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA  15213-3890