New SEI Course!

Practical Risk Management: Framework and Methods

September 23-24, 2009
Arlington, VA
Register at:
www.sei.cmu.edu/products/courses/p78.html
Organizations Need Software Product Lines Now More Than Ever!

Effectively using software product lines improves time to market, cost, productivity, and quality. They also enable rapid market entry and flexible response. And, using software product lines simplifies software maintenance and enhancement.
If you need to improve …
- the structure and behavior of your software-reliant systems (regardless of scale)
- your ability to predict that behavior

The SEI can…
- harness the appropriate technology to help you solve specific problems
- help you launch initiatives
- help you improve your capabilities
- conduct applied research that meets your needs
- partner with you to create leading edge techniques, methods, and tools

For more information contact info@sei.cmu.edu

Overview

Practicing strong information and cyber security is a nonnegotiable requirement for organizations doing business today. However, building security into an existing corporate culture is a complex undertaking. This series of podcasts provides both general principles and specific starting points for business leaders who want to launch an enterprise-wide security effort or make sure their existing security program is as good as it can be.

Please review our Legal Disclaimer

http://www.cert.org/podcast/
SEPG is the premier, global conference series on software and systems process management

http://www.sei.cmu.edu/sepg/index.html
Get Certified!

SEI Certifications:

Proof of your skill from a world leader in software engineering.

http://www.sei.cmu.edu/certification/
Want a Closer Connection to the SEI?

Become an SEI Member!

http://www.sei.cmu.edu/membership/
Do you have the knowledge you need?

SEI Education & Training

http://www.sei.cmu.edu/products/courses/
Biography: Christopher Alberts

Christopher Alberts is a senior member of the technical staff at the Software Engineering Institute. He is currently developing methods for managing systemic risk during the development and operation of software-intensive systems and systems of systems. Prior to his work in this area, he co-developed the OCTAVE® approach for managing information security risks and the Continuous Risk Management methodology for managing software development project risks. He has also co-authored two books, “Managing Information Security Risks: The OCTAVE℠ Approach” (Addison-Wesley 2002) and the “Continuous Risk Management Guidebook” (Software Engineering Institute 1996).
Biography: Audrey Dorofee

Audrey Dorofee is a senior member of the technical staff at the Software Engineering Institute. She is currently focused on the development and transition of advanced methods, tools and techniques for managing risk and opportunity in complex environments. She has co-authored two books, *Managing Information Security Risks: The OCTAVE<sup>SM</sup> Approach* (Addison-Wesley 2002) and the *Continuous Risk Management Guidebook* (Software Engineering Institute 1996).
Polling Question #1

Are you experienced in managing risk?

Answers:

- Yes – experienced in managing risks
- No – new to risk management
Mission Success in Complex Environments (MSCE) Project

Part of the SEI Acquisition Support Program (ASP), the MSCE Project develops methods, tools, and techniques for

• Advancing the state-of-the-practice for risk management
• Assuring success in complex, uncertain environments

The project builds on more than 17 years of SEI research and development in risk management.

• Continuous Risk Management for software-development projects
• Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) for organizational security
Topics

Mosaic Approach
Driver Analysis
Standard Set of Program Drivers
Risk Management Framework
Implementing Mosaic
Summary
Mosaic Approach
Widespread Use of Risk Management

Most programs and organizations implement some type of risk management approach when developing and operating software-intensive systems.

- Risk management plan
- Processes
- Tools

However, preventable failures continue to occur.

- Uneven and inconsistent application of risk-management practice
- Significant gaps in risk-management practice
- Ineffective integration of risk-management practice
- Increasingly complex management environment
### Rethinking Risk Management: A New Paradigm

<table>
<thead>
<tr>
<th>Traditional Paradigm</th>
<th>New Paradigm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing potential hazards</td>
<td>Achieving success</td>
</tr>
<tr>
<td>Tactical approach</td>
<td>Systemic approach</td>
</tr>
<tr>
<td><strong>Point solutions</strong></td>
<td></td>
</tr>
<tr>
<td>• Single type of risk (e.g., program, security, architecture)</td>
<td>• Multiple types of risk</td>
</tr>
<tr>
<td>• Single life-cycle phase</td>
<td>• Applicable across the life cycle</td>
</tr>
<tr>
<td>• Single entity (e.g., program, process, organization, system)</td>
<td>• Scalable to multi-enterprise, multi-system environments</td>
</tr>
</tbody>
</table>
Tactical and Systemic Approaches

Systemic View

Tactical View

Potential Event → Consequence → Condition

Potential Event → Consequence → Condition

Potential Event → Consequence → Condition

Potential Event → Condition

Impact on Objectives
**Mosaic**

*What*
An approach for managing risk and opportunity across the life cycle and supply chain

**Core Technologies**
- Assessment Methods
- Risk Management Framework

**Products and Services**
- Courses
- Workshops
- Course and Workshop Combinations
- Evaluations
Mosaic: *Focus on Assessment*

Every organization has preferred management practices.

The foundation of the Mosaic approach is a suite of methods for assessing risk continuously.

Mosaic also provides guidance for leveraging existing management practices to develop, implement, and track risk mitigation plans.
Mosaic assessments are modular in design.

Driver identification and analysis provide a common front end for multiple back-end analyses.
Mosaic: A Range of Analysis Options

Mosaic analysis methods range from basic to advanced.
Driver Analysis
A driver is a factor that has a strong influence on the eventual outcome or result.
Driver Framework

The driver framework is a common structure for classifying a set of drivers.
Drivers: **Success and Failure States**

A driver can guide the outcome toward key objectives (success state) or away from them (failure state).

- **Success State**
  - The process being used to develop (and deploy) the system is sufficient.

- **Failure State**
  - The process being used to develop (and deploy) the system is insufficient.
Mosaic provides an integrated view of the overall risk to key objectives.
# Basic Set of Drivers for Software Programs

<table>
<thead>
<tr>
<th></th>
<th>Driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Program Objectives</td>
</tr>
<tr>
<td>2</td>
<td>Plan</td>
</tr>
<tr>
<td>3</td>
<td>Process</td>
</tr>
<tr>
<td>4</td>
<td>Task Execution</td>
</tr>
<tr>
<td>5</td>
<td>Coordination</td>
</tr>
<tr>
<td>6</td>
<td>External Interfaces</td>
</tr>
<tr>
<td>7</td>
<td>Information Management</td>
</tr>
<tr>
<td>8</td>
<td>Technology</td>
</tr>
<tr>
<td>9</td>
<td>Facilities and Equipment</td>
</tr>
<tr>
<td>10</td>
<td>Organizational Conditions</td>
</tr>
<tr>
<td>11</td>
<td>Compliance</td>
</tr>
<tr>
<td>12</td>
<td>Event Management</td>
</tr>
<tr>
<td>13</td>
<td>Requirements</td>
</tr>
<tr>
<td>14</td>
<td>Design and Architecture</td>
</tr>
<tr>
<td>15</td>
<td>System Capability</td>
</tr>
<tr>
<td>16</td>
<td>System Integration</td>
</tr>
<tr>
<td>17</td>
<td>Operational Support</td>
</tr>
<tr>
<td>18</td>
<td>Adoption Barriers</td>
</tr>
<tr>
<td>19</td>
<td>Operational Preparedness</td>
</tr>
<tr>
<td>20</td>
<td>Certification and Accreditation</td>
</tr>
</tbody>
</table>
Driver questions are phrased from the success perspective. Probability is incorporated into the range of answers for each driver. The rationale for selecting an answer is recorded.
A simple analysis provides insight into current conditions.
Basic Risk Analysis: *Mission Risk*

<table>
<thead>
<tr>
<th>Mission Risk</th>
<th>Probability</th>
<th>Impact</th>
<th>Risk Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. The process being used to develop and deploy the system is insufficient.</td>
<td>High</td>
<td>Severe</td>
<td>High</td>
</tr>
</tbody>
</table>

Determined using results of driver analysis

Determined using standard risk analysis methods
A risk profile can be presented in relation to a framework or taxonomy.
Standard Set of Program Drivers
Driver Questions: Objectives

1. Program Objectives

- Are program objectives (product, cost, schedule) realistic and achievable?
Driver Questions: *Preparation*

2. **Plan**

   - Is the plan for developing (and deploying) the system sufficient?

3. **Process**

   - Is the process being used to develop (and deploy) the system sufficient?
Driver Questions: *Execution* -1

4. *Task Execution*
   - Are tasks and activities performed effectively and efficiently?

5. *Coordination*
   - Are activities within each team and across teams coordinated appropriately?

6. *External Interfaces*
   - Will work products from suppliers, partners, or collaborators meet the program’s quality and timeliness requirements?
Driver Questions: *Execution* -2

7. *Information Management*

- Is the program’s information managed appropriately?

8. *Technology*

- Does the program team have the tools and technologies it needs to develop the system and transition it to operations?

9. *Facilities and Equipment*

- Are facilities and equipment sufficient to support the program?
Driver Questions: *Environment*

10. *Organizational Conditions*

- Are enterprise, organizational, and political conditions facilitating completion of program activities?

11. *Compliance*

- Does the program comply with all relevant policies, laws, and regulations?
12. Event Management

- Does the program have sufficient capacity and capability to identify and manage potential events and changing circumstances?
Driver Questions: Result -1

13. Requirements
   • Are system requirements well understood?

14. Design and Architecture
   • Are the design and architecture sufficient to meet system requirements and provide the desired operational capability?

15. System Capability
   • Will the system satisfactorily meet its requirements?
Driver Questions: Result -2

16. System Integration

• Will the system sufficiently integrate and interoperate with other systems when deployed?

17. Operational Support

• Will the system effectively support operations?

18. Adoption Barriers

• Have barriers to customer/user adoption of the system been managed appropriately?
Driver Questions: \textit{Result -3}

19. \textit{Operational Preparedness}
   
   • Will people be prepared to operate, use, and maintain the system?

20. \textit{Certification and Accreditation}
   
   • Will the system be appropriately certified and accredited for operational use?
Polling Question #2

Do you use a risk management method that addresses all 20 driver questions?

Answers:

• Yes
• No
• Don’t know
Risk Management Framework
Mosaic: *Enabling Best Practice*

Mosaic also provides guidance for determining if an existing risk management practice is effective.

- The Risk Management Framework defines best practice for risk management.
- Mosaic provides approaches for evaluating a program’s risk management practice.
  - *Consistency Evaluation* – establishes whether key framework requirements are satisfied by a risk management practice
  - *Effectiveness Evaluation* – establishes the likelihood that a risk management practice will produce intended results (i.e., keep risk within an acceptable tolerance)
Risk Management Framework -1

Phase 1
Prepare for Risk Management

Phase 2
Perform Risk Management Activities

Phase 3
Sustain and Improve Risk Management Activities

Assess
Plan
Mitigate
The Risk Management Framework is implementation independent.

- Defines risk management activities
- Does not specify how to perform those activities

The framework provides a

- Foundation for a comprehensive risk management methodology
- Basis for improving a risk management practice
Polling Question #3

Is your current risk management practice effective?

Answers:

- Effective – all critical risks are being identified and mitigated; no unexpected, critical problems
- Needs improvement – some critical problems are showing up that should have been caught as risks
- Not very helpful – information not used by managers making decisions
- Just a check-the-box process because we have to do it
- Don’t know
Implementing Mosaic
Ways of Implementing Mosaic

Improve an existing risk management practice using the Risk Management Framework

Adopt one of Mosaic’s assessment methods

- Select the appropriate assessment “platform” (basic to advanced)
- Tailor drivers and artifacts based on mission and objectives

Use Mosaic to integrate risk information in a multi-enterprise environment
Mosaic: An Integrated Decision-Making Approach

Decision-Making Data

Back-End Analysis

Driver Analysis

Systemic View

Tactical View

Positive Conditions
Negative Conditions
Potential Events with Positive Consequences
Potential Events with Negative Consequences

Strengths
Weaknesses/Issues
Tactical Opportunities
Tactical Risks
Extending Driver Analysis

Driver analysis provide a foundation for program decision making.

Mosaic also includes a variety of back-end analyses for more in-depth evaluation of drivers.

- Gap analysis (*Mission Diagnostic*)
- Basic risk analysis (*Risk Diagnostic*)
- Intermediate risk analysis
- Mission success analysis
- Integrated risk and opportunity analysis
- Risk simulation models
- Others

<table>
<thead>
<tr>
<th>Gap Analysis</th>
<th>Basic Risk Analysis</th>
<th>Intermediate Risk Analysis</th>
<th>Mission Success Analysis</th>
<th>Integrated Risk and Opportunity Analysis</th>
<th>Mission Assurance Analysis</th>
<th>Risk Simulation Models</th>
<th>Other Types of Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver Analysis</td>
<td>Driver Identification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mosaic in Multi-Enterprise Environments

Programs that cross multiple organizational boundaries require a systemic viewpoint when managing risk.

- Acquire and maintain a broad view of the risk to program objectives
- Avoid local optimization of risk
- Keep volume of risk data to a manageable level
Integrated View of Risk in Multi-Enterprise Environments

SEI Mosaic

SEI Continuous Risk Management

Proprietary Risk Management
Summary
Mosaic Assessments: Key Characteristics

Straightforward and easy to apply
Comprehensive, holistic view of a program’s risk drivers
Fully scalable to multi-system and multi-enterprise environments
Easily integrated with existing management practices
Success oriented
Systemic, top-down analysis
Mosaic Assessments: *Application in Multiple Domains*

Program risk management
Mission and software assurance
Information technology (IT) management
Data management
Cyber-security management
Business process management
Critical infrastructure protection
Others
Potential Areas of Future Research

Metrics
Risk-based improvement
Modeling and simulation
Mosaic Resources

SEI web pages http://www.sei.cmu.edu/risk/

• Twenty Questions for Program Managers
• Presentations
• Technical Reports
  – A Framework for Categorizing Key Drivers of Risk
  – Mission Diagnostic Protocol, Version 1.0: A Risk-Based Approach for Assessing the Potential for Success
Mosaic: Portfolio -1

Courses

• Risk Management Framework: Best Practices in Risk Management
• Introduction to Practical Risk Management
• Practical Risk Management: Framework and Methods

Workshops

• Risk Management Tailoring and Improvement Workshops

Course and Workshop Combinations
Mosaic: *Portfolio* -2

**Evaluations**

- Systemic Risk Evaluation
- Mission Success Evaluation
- Risk Management Framework Evaluation
- Custom Evaluation
Focus of Mosaic Products and Services

Basic Analysis

Gap Analysis
Basic Risk Analysis
Intermediate Risk Analysis
Mission Success Analysis
Integrated Risk and Opportunity Analysis
Mission Assurance Analysis
Risk Simulation Models

Courses and Workshops

Evaluations

Research and Development

Advanced Analysis
Public Training in September 2009

Practical Risk Management: Framework and Methods

- September 23-24, 2009
- SEI office in Arlington, VA
For Additional Information

Christopher Alberts  
Email: cja@sei.cmu.edu  
Phone: 412-268-3045  
Fax: 412-268-5758

Audrey Dorofee  
Email: ajd@sei.cmu.edu  
Phone: 412-268-6396  
Fax: 412-268-5758

WWW  
http://www.sei.cmu.edu/risk/

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