Software And Systems Engineering Risk Management

John Walz
VP Technical and Conferences Activities, IEEE Computer Society
Vice-Chair Planning, Software & Systems Engineering Standards Committee, IEEE Computer Society
US TAG to ISO TMB Risk Management Working Group

Systems and Software Technology Conference, SSTC 2010
**Software And Systems Engineering Risk Management**

**IEEE Computer Society, 2001 L Street N.W., Suite 700, Washington, DC, 20036-4928**

**Presented at the 22nd Systems and Software Technology Conference (SSTC), 26-29 April 2010, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License**

**Approved for public release; distribution unlimited**

**Same as Report (SAR)**

**32**

**Standard Form 298 (Rev. 8-98)**

Prescribed by ANSI Std Z39-18
Agenda

• What is the change in Risk?
• What are the other Risk definitions?
• What is Risk Management (RSKM)?
• What are the other RSKM standards?
• Where is RSKM in the enterprise and project?
• RSKM in Software and System Technology (SST) supply chain?
• What are the RSKM processes?
• What is the RSKM standards history?
• What changed in RSKM?
• What can you do?
"change the game"

• This year, the Systems and Software Technology Conference will explore various technologies which are expected to make abrupt changes to common thought. We will explore the tools, the **processes**, and the **ideas** which will "change the game" and make the way we have done things in the past - obsolete.

• The DOD supply chain has implements risk management processes to meet customer needs for the major objectives of timely delivery of functionality with quality. As software and systems complexity increased, these objectives have been difficult to achieve together. During system operations, unknown quality issues and events have placed missions at risk.

• What’s changing the game are coordinated standards issued late in 2009:
  
  • **Risk management** — Principles and guidelines
  • **Risk management** — **Vocabulary**
  • **Risk management** — **Risk Assessment**
### Changed Risk definition

<table>
<thead>
<tr>
<th>Published</th>
<th>RSKM Vocabulary, ISO Guide 73</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>combination of the probability of an event and its consequence</td>
</tr>
<tr>
<td>2009</td>
<td>effect of uncertainty on objectives</td>
</tr>
</tbody>
</table>

This is where ISO 31000 is clearly different from existing guidelines in that the emphasis is shifted from something happening – the event – to the effect on objectives.

*Kevin W. Knight*
RSMK Concepts from New Zealand Society for Risk Management

• RSMK concepts which underpin both
  – AS/NZS4360:2004 and
  – ISO 31000:2009

• Risk defined as "the effect of uncertainty on objectives"
  – The change in definition shifts the emphasis
    from "the event" (something happens)
    to "the effect" which is the effect of the event on objectives.

So, the "risk" isn't the chance of having a fire (for example) but the chance that value will be destroyed and or income flow disrupted (assuming preserving value and income flow was part of the objective).

• http://www.risksociety.org.nz/what_is_risk_management
What are the other Risk definitions?
**risk** — effect of uncertainty on objectives, Guide 73-2009

- **NOTE 1** An effect is a deviation from the expected — positive and/or negative.
- **NOTE 2** Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
- **NOTE 3** Risk is often characterized by reference to potential events and consequences, or a combination of these.
- **NOTE 4** Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
- **NOTE 5** Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
risk management, risk management process, establishing the context, & risk assessment

Guide 73-2009

• risk management — coordinated activities to direct and control an organization with regard to risk

• risk management process — systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk

• establishing the context — defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy

• risk assessment — overall process of risk identification, risk analysis and risk evaluation.
What is Risk Management (RSKM)?
Risk management — Principles and Guidelines
ISO 31000:2009

• Provides principles and generic guidelines on risk management

• Can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000 is not specific to any industry or sector

• Can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and asset

• Can be applied to any type of risk, whatever its nature, whether having positive or negative consequences

• Although provides generic guidelines, it is not intended to promote uniformity of risk management across organizations

  • Design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed

• Utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards

• Not intended for the purpose of certification
ISO 31000 Risk management
Principles / Benefits

• For risk management to be effective, an organization should at all levels comply with the principles below.
  • creates and protects value
    • contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation
  • is an integral part of all organizational processes
  • is part of decision making
  • explicitly addresses uncertainty
  • is systematic, structured and timely
  • is based on the best available information
  • is tailored
  • takes human and cultural factors into account
  • is transparent and inclusive
  • is dynamic, iterative and responsive to change
  • facilitates continual improvement of the organization
RSKM Framework

Mandate and commitment

Design of framework for managing risk
• Understanding of the organization and its context
• Establishing risk management policy
• Accountability
• Integration into organizational processes
• Resources
• Establishing internal communication and reporting mechanisms
• Establishing external communication and reporting mechanisms

Continual improvement of the framework

Implementing risk management
• Implementing the framework for managing risk
• Implementing the risk management process

Monitoring and review of the framework
Risk management process

- Establishing the context
- Communication and consultation
- Risk assessment
  - Risk identification
  - Risk analysis
  - Risk evaluation
- Risk treatment
- Monitoring and review

IS 31010
RSKM Maturity

level 0. **Pay out** for risk occurrences (insurance premiums & payouts)

level 1. **Test** in risk detection & mitigation (verification / validation)

level 2. **Design** in risk aversion (preventative action)

good
Risk assessment techniques
IEC/ISO 31010:2009

• Answer the following fundamental questions:
  • what can happen and why (by risk identification)?
  • what are the consequences?
  • what is the probability of their future occurrence?
  • are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?
  • is the level of risk tolerable or acceptable and does it require further treatment?

• Provides input to decisions about:
  • whether an activity should be undertaken;
  • how to maximize opportunities;
  • whether risks need to be treated;
  • choosing between options with different risks;
  • prioritizing risk treatment options;
  • the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level.
Benefits of performing risk assessment, IEC/ISO 31010

- understanding the risk and its potential impact upon objectives;
- providing information for decision makers;
- contributing to the understanding of risks, in order to assist in selection of treatment options;
- identifying the important contributors to risks and weak links in systems and organizations;
- comparing of risks in alternative systems, technologies or approaches;
- communicating risks and uncertainties;
- assisting with establishing priorities;
- contributing towards incident prevention based upon post-incident investigation;
- selecting different forms of risk treatment;
- meeting regulatory requirements;
- providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria;
- assessing risks for end-of-life disposal.
Risk Assessment, IEC/ISO 31010

- Expands Risk analysis:
  - Controls assessment
  - Consequence analysis
  - Likelihood analysis and probability estimation
  - Preliminary analysis
  - Uncertainties and sensitivities

* from ISO 31000
What are the other RSKM standards?
## Standards addressing RSKM from Technical Committees

<table>
<thead>
<tr>
<th>Technical Area</th>
<th>Committee</th>
<th>Std #</th>
<th>Standards title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td>ISO TMB</td>
<td>Guide 73</td>
<td>Risk Management Vocabulary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO 31000</td>
<td>Risk Management Principles &amp; Guidance</td>
</tr>
<tr>
<td>Dependability</td>
<td>IEC TC 56</td>
<td>IEC/ISO 31010</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Software &amp; System Engineering</td>
<td>JTC1/SC7</td>
<td>IS 12207</td>
<td>Software Engineering Life Cycle Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IS 15288</td>
<td>Systems Engineering Life Cycle Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IS 16085</td>
<td>Risk Management Process</td>
</tr>
<tr>
<td>Quality</td>
<td>ISO TC 176</td>
<td>ISO 9001</td>
<td>Quality Management System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO 9000</td>
<td>Quality Management Vocabulary</td>
</tr>
<tr>
<td>Environment</td>
<td>ISO TC 207</td>
<td>ISO 14001</td>
<td>Environmental Management System</td>
</tr>
<tr>
<td>IT Security</td>
<td>JTC1/SC22</td>
<td>IS 27005</td>
<td>Information Security RSKM</td>
</tr>
<tr>
<td>Supply Chain Security</td>
<td>ISO TC 8</td>
<td>ISO/PAS 28001</td>
<td>Security management systems for the supply chain</td>
</tr>
<tr>
<td>Societal security</td>
<td>ISO TC 223</td>
<td>ISO/PAS 22399</td>
<td>Guideline for incident preparedness and operational continuity management</td>
</tr>
<tr>
<td>Medical Devices</td>
<td>ISO TC 210</td>
<td>ISO 14971</td>
<td>Application of risk management to medical devices</td>
</tr>
</tbody>
</table>
Where is RSKM in the enterprise and project?
Governance Risk Compliance (GRC)

VOLUNTARY BOUNDARY
boundary defined by management including public commitments, organizational values, contractual obligations, and other voluntary policies

BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives

OBSTACLES
obstacles impede progress toward achieving objectives

OBJECTIVES
strategic, operational, customer, compliance and reporting objectives

MANDATED BOUNDARY
boundary established by external forces including laws, government regulation and other mandates

Open Compliance & Ethics Group (OCEG)
Risk Management in SST organization

- Enterprise
- GRC
- 31000
- 31010
- Products & services
- 15288/12207
- 16085
- Supply chain management
Enterprise vs. Project

- The management of risk extends from devices to enterprise systems, from quality management, to project management, to product development, and to system operations.


RSKM in Software and System Technology (SST) supply chain?
Standards affecting SST supply chain

• S2E Life Cycle Processes
  IEEE/ISO/IEC 12207/15288

• Risk Management Processes

• Risk management — Principles and Guidelines
  ISO 31000:2009

• Risk management -- Risk assessment techniques
  IEC/ISO 31010:2009

• Risk management — Vocabulary
  Guide 73:2009
What are the RSKM processes?
What is the RSKM standards history?
## Risk Management (RSKM) Standards – Selected History

<table>
<thead>
<tr>
<th>Year</th>
<th>Std #</th>
<th>Std Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>AS/NZS 4360</td>
<td>RSKM</td>
</tr>
<tr>
<td>1999</td>
<td>AS/NZS 4360</td>
<td>RSKM</td>
</tr>
<tr>
<td>2001</td>
<td>JIS Q 2001</td>
<td>Guidelines for Development and Implementation of RSKM System</td>
</tr>
<tr>
<td>2001</td>
<td>IEEE 1540</td>
<td>Software Life Cycle Processes – RSKM</td>
</tr>
<tr>
<td>2001</td>
<td>IEC 62198</td>
<td>Project RSKM – Application Guidelines</td>
</tr>
<tr>
<td>2004</td>
<td>AS/NZS 4360</td>
<td>RSKM</td>
</tr>
<tr>
<td>2004</td>
<td>COSO</td>
<td>Enterprise RSKM Framework</td>
</tr>
<tr>
<td>2006</td>
<td>ISO/IEC 16085</td>
<td>Risk Management Process</td>
</tr>
<tr>
<td>2008</td>
<td>ISO/IEC 12207</td>
<td>Software Lifecycle Processes</td>
</tr>
<tr>
<td>2009</td>
<td>ISO 31000</td>
<td>Risk management – Principles and guidelines</td>
</tr>
</tbody>
</table>
Where can you do?
ISO 31000 Implementation

- The SST supply chain’s practice of risk management must be reexamined to
  - include the positive “opportunity” with the negative view of risk
  - expand application of risk to any organizational objective
  - expand risk management to the enterprise
  - carefully define their “Context” as there is little guidance
  - integrate RSKM into their ISO 9001 clause 8.5.3 Preventive action
- avoid offers for conformity assessments
- use 16085 for product & service development and deployment