PSM 2001 Aspen, Colorado

Paul R. Croll
Chair, IEEE SESC
Computer Sciences Corporation
pcroll@csc.com
Objectives

- Describe Risk Management in the context of a life cycle process framework
- Describe IEEE 1540’s Risk Management process model and process requirements
- Describe other Standards that complement IEEE 1540 in managing risk in the acquisition and engineering of software intensive systems
Risk Management (RM) in the Life Cycle Context

- An organizational life cycle process
  - responsibility of the organization using the process
  - the organization ensures that the process exists and functions

- IEEE Standard 1540 assumes that the other management and technical processes of IEEE/EIA 12207 perform the treatment of risk
IEEE/EIA 12207 Life Cycle Process Tree

Source: Singh97

Risk Management touched on in 12207
Risk Management focused on in 12207
Risk Management Objectives in IEEE/EIA 12207

- Sprinkled throughout the Acquisition, Supply, Development, Operation, Verification, Joint Review, Problem Resolution, and Tailoring Processes

- Focused on in *Management Process* objectives
  - Determine scope of risk management to be performed
  - Identify risks to the project as they develop
  - Analyze risks
  - Determine mitigation priority
  - Define, implement and assess mitigation strategies
  - Define, apply and assess risk metrics
IEEE/EIA 12207 Process Interactions

Source: Singh97
IEEE/EIA 12207 Process Roles

**ACQUISITION ROLE**
- **ACQUIRER**
  - **ACQUISITION PROCESS**
  - **ACQUIRER**

**SUPPLY ROLE**
- **SUPPLIER**
  - **SUPPORTING PROCESSES**
  - **SUPPORTING PROCESSES**

**OPERATING ROLE**
- **OPERATOR**
  - **OPERATION PROCESS**
  - **OPERATION PROCESS**

**ENGINEERING ROLE**
- **DEVELOPER**
  - **MAINTAINER**
  - **MAINTENANCE PROCESS**

**SUPPORTING ROLE**
- **EMPLOYER OF SUPPORTING PROCESSES**
- **ORGANIZATIONAL ROLE**
  - **MANAGER**
  - **ORGANIZATIONAL PROCESSES**

**PROCESS**
- **DEVELOPMENT PROCESS**
  - **DEVELOPMENT PROCESS**

**SUPPLY PROCESS**
- **SUPPLY PROCESS**
  - **SUPPLY PROCESS**

**OPERATION PROCESS**
- **OPERATION PROCESS**
  - **OPERATION PROCESS**

**MAINTENANCE PROCESS**
- **MAINTENANCE PROCESS**
  - **MAINTENANCE PROCESS**

**SUPPRTING PROCESSES**
- **SUPPORTING PROCESSES**
  - **SUPPORTING PROCESSES**

**Source:** Singh97
Risk Management Process Overview

1. Technical and Management Processes
   - Perform Risk Treatment
2. Plan and Implement Risk Management
3. Manage the Project Risk Profile
4. Perform Risk Analysis
5. Perform Risk Monitoring
6. Evaluate the Risk Management Process
7. Improve Risk Management

Source: IEEE Standard 1540:2001 © IEEE 2001. All rights reserved.
Risk Management Process Overview

- Define the information requirements for RM
  - information needed and priority
  - risk areas of concern
  - RM policies required
  - risk acceptability thresholds
- Make decisions regarding risks
- Make recommendations for improving the RM process

Source: IEEE Standard 1540:2001 © IEEE 2001. All rights reserved.
• Establish RM policies to support information required by decision makers
  – how RM is to be performed
  – tools or techniques to be used
  – how RM activities will be coordinated
  – how risk is to be communicated

• **Establish the RM process**
• Establish responsibility for RM
• Assign RM resources
• **Establish RM process evaluation**

---

**Source:**
IEEE Standard 1540:2001
All rights reserved.
Risk Management

Overview

- Create a consistent current and historical view of the risks present and their treatment
- Define the technical and managerial risk management context
  - risks areas of concern
  - stakeholder(s) perspective(s)
  - objectives, assumptions and constraints
- Establish risk thresholds
- Establish and maintain the project risk profile
- Communicate risk status to stakeholders

Plan and Implement Risk Management

Evaluate the Risk Management Process

Source: IEEE Standard 1540:2001 © IEEE 2001. All rights reserved.
• Identify risks defined by RM context
• Estimate risk likelihood and consequences
• Evaluate and prioritize the risks and their interactions against thresholds
• Recommend risk treatment where applicable
• Document in risk action request
  – measures of treatment effectiveness
  – contingency plans

Source: IEEE Standard 1540:2001© IEEE 2001. All rights reserved.
Risk Management Process Overview

- Management evaluates risk action requests and determines acceptability of risks
- If risk reduction actions are to be taken, management selects, plans, monitors, and controls treatment to decrease risk exposure

Source: IEEE Standard 1540:2001 © IEEE 2001. All rights reserved.
Once a risk treatment has been selected
– if a 12207 Life Cycle Process is employed,
  + risk treatment is managed using the problem management approach of the Management Process
– if a non-12207 Life Cycle Process is employed,
  + a detailed Risk Treatment Plan must be developed and implemented
Risk Management Process Overview

1. Technical and Management Processes
2. Plan and Implement Risk Management
3. Manage the Project Risk Profile
4. Perform Risk Treatment
5. Perform Risk Monitoring
6. Evaluate the Risk Management Process
7. Improvment Actions

- Review and update individual risk states and the management context
- Assess effectiveness of risk treatments
- Seek out new risks

Source: IEEE Standard 1540:2001 © IEEE 2001. All rights reserved.
Risk Management Process
Overview

- Capture RM information
- Assess and improve the RM process
  - collect RM information
  - assess the quality of the process
  - identify opportunities for improvement
  - provide feedback to management
  - make improvements to the process
- Generate lessons learned

Source:
IEEE Standard
1540:2001
All rights reserved.
IEEE 1540 and ISO/IEC 15026

ISO/IEC 15026:1998, Information Technology — System and Software Integrity Levels

- Defines a process for establishing integrity levels that are used to contain risk within acceptable values
  - the system integrity level reflects the worst case risk that is associated with the as-designed system
  - all appropriate risk dimensions are addressed
- Requires employment of a risk management process
IEEE 1540 and ISO/IEC 15939

- ISO/IEC 15939:FDIS, Information Technology —Software Measurement Process
  - Identifies the activities and tasks that are necessary to successfully identify, define, implement, and improve a software measurement process
    - Two core activities
      - Plan the Measurement Process
      - Perform the Measurement Process
    - Two supporting activities
      - Establish and Sustain Measurement Commitment
      - Evaluate Measurement
IEEE 1540 and ISO/IEC 15939 - 2

- References to risk in ISO/IEC 15939
  - Plan the Measurement Process
    - Identify Information Needs
  - Annex A: The measurement information model
    - Measurable Concept
IEEE 1540 and IEEE 1012

  - Uses integrity levels to determine appropriate V&V activities
  - These integrity levels could be determined in the baseline risk profile
IEEE 1540 and IEEE 1228

  - Addresses planning for a software safety program that provide a systematic approach to reducing software risks
    - Requires that a risk assessment be performed to identify potential safety risks
    - Requires that risk treatment alternatives be addressed for uncontrolled risks
IEEE 1540 and IEEE 1058

  - requires the specification of a risk management plan
    - identification, analysis and prioritization of project risk factors
    - procedures for contingency planning, risk monitoring, and changes in risk status
IEEE 1540 and IEEE 982.1 and 982.2

  - measures appropriate for use in risk management

  - guidance regarding measures appropriate for use in risk management
For more information . . .

Paul R. Croll  
Computer Sciences Corporation  
5166 Potomac Drive  
King George, VA 22485-5824

Phone: +1 540.663.9251  
Fax: +1 540.663.0276  
e-mail: pcroll@csc.com

For IEEE Standards:  
http://standards.ieee.org/catalog/  
For the IEEE Software Engineering Standards Committee:  
http://computer.org/standard/sesc/
Questions?
References


References - 2


