Lecture 11

➔ (Week 11 - March 18, 2024)

Requirements Change Factors:

- Requirements errors, conflicts, and inconsistencies may be detected at any phase of the project.
- Evolving customer/user knowledge leads to a better understanding of their needs over time.
- Technical, schedule, or cost problems may require revisiting and adapting the requirements.

Changing Customer Priorities:

- Customer priorities may change due to shifts in the system environment, business goals, competition, laws, regulations, technology, or organizational structure.
- These changes necessitate adjustments to the project's requirements.

Requirements Stability Vs. Volatility:

- Stable (enduring) requirements pertain to the essence of the system and its domain, changing slowly.
- Volatile requirements are specific to the system's instantiation in a particular environment and may change rapidly.

Types of Volatile Requirements:

- Mutable requirements change due to shifts in the system's operating environment.
- Emergent requirements arise during system design and implementation.
- Consequential requirements are based on assumptions about system usage, some of which may prove wrong.
- Compatibility requirements depend on other equipment, technology, or processes.

Expectations of Requirements Management:

1. Identification of individual requirements.
2. Traceability from highest-level requirements to implementation.
3. Impact assessments of proposed changes.
4. Controlled access to current project information.
5. Change control and deployment of required tool support.

Identification of Requirements:

- Each requirement should have a unique identification.
- Common approaches include requirements numbering, but this may lead to ambiguity until the document is complete.

Backward and Forward Traceability:

- **Forward-to Traceability:** Links documents preceding the requirements document to relevant requirements, aiding validation and assessing changes to users' needs.
- **Forward-from Traceability:** Links requirements to design and implementation components, ensuring all requirements are satisfied.
- **Backward-to Traceability:** Links design and implementation components back to requirements, helping determine the rationale behind each item's design/implementation.
- **Backward-from Traceability:** Links requirements to their sources in other documents or people, assisting in validation and evaluating the impact of requirement changes.

Types of Traceability:

- **Requirements – Source Traceability:** Links requirements with a person or document.
- **Requirements – Rationale Traceability:** Links requirements with their justification.
- **Requirements – Requirements Traceability:** Links requirements with other requirements dependent on them.
- **Requirements – Architecture Traceability:** Links requirements with the subsystems where they are implemented.

- **Requirements – Design Traceability:** Links requirements with specific hardware or software components.
- **Requirements – Interface Traceability:** Links requirements with external system interfaces.
- **Requirements – Feature Traceability:** Links requirements with corresponding system features.
- **Requirements – Tests Traceability:** Links requirements with test cases verifying them.
- **Requirements – Code Traceability:** Infers links between requirements and implemented code.

Representation of Traceability:

- **Traceability Table:** Shows relationships between requirements or between requirements and other artifacts.
- **Traceability Matrix:** Defines links between pairs of elements and their relationships, more amenable to automation.
- **Traceability List:** Simplified form of a traceability matrix, useful for managing large numbers of requirements.

Traceability Planning:

- Stakeholder identification and needs analysis.
- Defining useful, measurable, and feasible objectives.
- Definition of links, attributes, and automation possibilities.
- Establishing processes, roles, and access for collecting and updating traceability information.
- Addressing exceptional situations and establishing traceability policies.

Tool Support for Change Management:

- Tool facilities may include electronic change request forms, databases, change models, electronic transfer of forms, electronic signatures, discussion forums, and direct links to requirements databases.
- Requirements management tools facilitate change management processes.

What Kind of Tool Do We Need?

- Various tools are available, including word processors, spreadsheets, commercial RM tools (e.g., IBM DOORS, Telelogic Requisite Pro), internal tools (e.g., GenSpec), open-source RM tools (e.g., OSRMT), bug tracking tools (e.g., Bugzilla), and collaboration tools (e.g., TWiki).

What Should We Look For in a Tool?

- Attributes for requirements and links, version and change management, database repository, traceability, analysis capabilities, automatic inspection of requirements, visualization and reports, requirements document generation, monitoring of requirement statuses, access control, import/export features, communication with stakeholders, scripting language for automation, and support for reuse of requirements, models, and projects.

RM Tool Architecture - Example:

- Illustrates integration of requirements management with project-tracking, project estimation, version control, design modeling, test management, and change-request tools.

Definitions:

- **Risk:** Probability of incurring net loss while pursuing a goal.
- **Positive Risk (Opportunity):** Pursuing a potential gain, which may result in net gain or loss.
- **Reducible Risk:** Predictable or controllable risks that can be mitigated.
- **Irreducible Risk:** Unpredictable or uncontrollable risks, including unpredictable or beyond-control events such as terrorist acts or natural disasters.
- Note: Irreducible risks are handled through business continuity practices.

Elements of Risk Management:

1. **Risk Management Planning:** Establishing the overall approach to risk management for the project, including roles and responsibilities, methodologies, and tools to be used.
2. **Risk Identification:** Systematically identifying potential risks that could affect the project's objectives.
3. **Qualitative Risk Analysis:** Assessing the likelihood and impact of identified risks qualitatively, often using techniques such as probability and impact matrices or risk scoring.

4. **Quantitative Risk Analysis:** Further analyzing risks by assigning numerical values to the probabilities and impacts, allowing for more precise risk assessment.
5. **Risk Prioritization:** Ranking risks based on their severity and likelihood to determine which ones require immediate attention and mitigation.
6. **Risk Response Planning:** Developing strategies and action plans to address identified risks, including risk mitigation, avoidance, transfer, or acceptance.
7. **Risk Monitoring:** Continuously tracking identified risks throughout the project lifecycle to ensure that mitigation measures remain effective and that new risks are promptly addressed.
8. **Risk Control:** Taking corrective actions as needed to mitigate risks, prevent them from escalating, and ensure that the project stays on track.
9. **Tracking & Auditing (Risk History):** Maintaining a record of all identified risks, their responses, and the outcomes of those responses for future reference and audit purposes.
10. **Evaluate & Revise:** Regularly reviewing the effectiveness of risk management processes and making necessary adjustments based on lessons learned and changing project conditions.

Risk Categorizes:

- **Known Risks:** Identifiable risks based on careful evaluation of project plans, environments, and reliable information sources. These risks can be estimated and managed through response plans.
- **Predictable Risks (but unknown risks):** Risks extrapolated from past projects, where probability of occurrence is known but precise impact is uncertain. Contingency plans can help mitigate these risks.
- **Unpredictable Risks:** Hard-to-predict risks that are outside historical or probabilistic models, often referred to as "Joker" risks.
- **Unknowable Risks:** Risks beyond the scope of risk management, such as corporate failures or natural disasters, usually addressed by crisis management.