Module 8

Software Quality Concepts, Assurance, Security Engineering, and Testing

---

▼ What are the key attributes of quality software?

- Effectiveness
  - An effective software process establishes the infrastructure that supports any effort at building a high-quality software product.
- Usefulness
  - A useful product delivers the content, functions, and features that the end user desires, but as important, it delivers these assets in a reliable, error-free way.
  - A useful product always satisfies those requirements that have been explicitly stated by stakeholders.
  - In addition, it satisfies a set of implicit requirements (e.g., ease of use) that are expected of all high-quality software.
- Adds value
  - By adding value for both the producer and user of a software product, high-quality software provides benefits for the software organization and the end-user community.
  - The software organization gains added value because high-quality software requires less maintenance effort, fewer bug fixes, and reduced customer support.
  - The user community gains added value because the application provides a useful capability in a way that expedites some business process.

    - The end result is (1) greater software product revenue, (2) better profitability when an application supports a business process, and/or (3) improved availability of information that is crucial for the business.

▼ What activities are involved in software quality assurance (SQA)?

- Standards: ensure that standards are adopted and followed, and that the system or product conforms to them.
- Audits: audits are reviews performed by SQA personnel to make sure that quality guidelines are being followed. For example, an audit of the technical review process might be performed to make sure the reviews are being done effectively.
- Testing: the job of SQA is to make sure that testing is done properly.
- Error/defect collection and analysis: SQA collects and analyzes error and defect data to understand how errors were made in order to improve future design, coding, and testing.
- Change management: SQA makes sure the adequate change management practices have been implemented.
- Education: it is the role of the SQA organization to lead software process improvement initiatives and to promote and sponsor educational programs.
- Vendor management: three types of software are purchased from external software vendors: shrink-wrapped packages (e.g., Microsoft Office), a customized basic skeletal structure prepared for future internal refinement, and contracted software development. The SQA team should be involved in the contracting process with vendors to makes sure quality practices have been implemented.
- Security management: SQA checks to make sure that the correct processes and technology are in place for software security management.
- Safety: SQA may be asked to assess the impact of software failure and to define ways to maximize safety.
- Risk management: Although the analysis and mitigation of risk is the responsibility of software engineers, the SQA organization makes sure that risk

management activities are properly performed and that contingency plans are in place.

▼ What's involved in the RMF (NIST Risk Management Framework) security assessment method?

- Categorize the information system and the processes stored and transmitted by the system using an impact analysis.
- Select a preliminary set of baseline security controls for the system based on the level of security needed. Use a risk assessment to determine how to customize the security controls as needed.
- Implement the security controls and describe how the controls are employed within the information system and its operational environment.
- Assess the security controls with relevant assessment procedures to determine whether the controls have been implemented correctly and are working as expected.
- Authorize the information system operation based on a determination of the risk to organizational operations and assets, individuals, or other organizations (including national defense), from the operation of the information system that this risk is acceptable.
- Monitor the security controls in the information system on an ongoing basis. This includes assessing the effectiveness of the controls, documenting changes made to the system or operational environment, exploring the security impact of those changes, and reporting any security concerns to management.

▼ What is threat modeling?

Threat modeling is a way to create an abstraction of a software system that identifies attackers' abilities and goals, and then using that abstraction to determine possible threats that the system must address.

▼ What's covered by STRIDE (threat categories)?

- Threat: Spoofing. Security property: Authentication.
- Threat: Tampering. Security property: Integrity.
- Threat: Repudiation. Security property: Nonrepudiation.

- Threat: Information disclosure. Security property: Confidentiality.
- Threat: Denial of service. Security property: Availability.
- Threat: Elevation of privilege. Security property: Authorization.

▼ What is verification?

The evaluation of work products of a phase of development to determine whether they meet the specified requirements for that phase.

▼ What is the objective of verification?

To make sure the product is being developed according to design specifications and requirements.

▼ What is validation?

The evaluation of software at the end of the development process to determine whether they meet the business needs.

▼ What is the objective of validation?

To make sure the product actually meets user needs and that these needs were understood correctly in the first place.