Case Study: Integration of Security (ISO 27001) and Software Quality (ISO 9001 / ISO 25010)

1. Security as a Quality Attribute

Security is a primary quality characteristic according to ISO/IEC 25010. ISO 27001 provides the management framework for achieving and maintaining this capability, ensuring that information is protected and risks are managed proactively.

2. Integration Points in the Software Development Lifecycle (SDLC)

- **Requirements:** Security user stories, threat modeling, and acceptance criteria.
- **Coding:** Secure engineering principles, use of SAST/DAST tools to ensure clean, vulnerability-free code.
- **Testing:** Security test cases, penetration testing, and validation of implemented controls.
- **Deployment:** Change management, security validation in CI/CD pipelines.

3. Threat Modeling Example (STRIDE)

STRIDE is a framework for classifying and understanding threats: - **Spoofing:** Authentication threats (e.g., phishing, credential theft). - **Tampering:** Integrity threats (e.g., unauthorized data modification). - **Repudiation:** Lack of audit trails (e.g., denial of actions). - **Information Disclosure:** Confidentiality threats (e.g., data leaks). - **Denial of Service:** Availability threats (e.g., DDoS attacks). - **Elevation of Privilege:** Authorization threats (e.g., privilege escalation).

Example: For a password reset feature, mitigations include rate limiting, secure token generation, encryption at rest, and secure email delivery.

4. Audit Format (Verification & Action)

- **General Information:** Audit scope, objectives, and participants.
- **Methodology & Criteria:** Standards used (ISO 27001, ISO 25010), verification methods.
- **Executive Summary:** Overall compliance level, key findings.
- **Detailed Findings:** Non-conformities, risks, and improvement opportunities.
- **Corrective Actions:** Recommendations and action plans.

5. Corrective Action Plan (CAP) Template

- **Action Details:** Description, responsible party, deadline.
- **Follow-up:** Verification of effectiveness and closure.

This document is provided as a practical resource for understanding and applying ISO 27001 in software projects. For more details, visit the app or contact your quality manager.