GRC Security Validation Guideline for Software Evaluation

Author: Timothy G. Majerus

@thetimmajerus

Overview:

This document is a general guideline of the GRC practices for evaluation of software before purchase and or implementation for standard and rigorous security practices. This document should be used by the evaluators in conjunction with a questionnaire presented to the software team / vendor. Below is a basic overview of an evaluation questionnaire with answers.

Question: How does the software ensure data encryption both at rest and in transit?

Answer: *The software should use industry-standard encryption protocols like AES-256 for data at rest and TLS 1.2 or higher for data in transit.*

Question: What are the access control mechanisms in place?

Answer: *The software must support role-based access control (RBAC / ABAC), multi-factor authentication (MFA), and provide detailed logs for access events.*

Question: Is there a compliance certification or audit the software has undergone? (e.g., SOC 2, ISO 27001)

Answer: *The software should have certifications or have undergone audits like SOC 2 Type II or be compliant with ISO 27001 standards.*

Question: How does the software handle vulnerability management?

Answer: *It should include regular vulnerability assessments, patch management processes, and an incident response plan.*

Question: Can the software integrate with existing GRC tools or platforms?

Answer: *It should offer APIs or pre-built integrations with major GRC platforms like RSA Archer, ServiceNow, or others for seamless workflow.*

Question: What measures are in place for data backup and disaster recovery?

Answer: *There must be robust data backup solutions, regular testing of disaster recovery plans, and off-site storage options.*

Question: How does the software support regulatory compliance (e.g., GDPR, HIPAA)?

Answer: *The software should provide features or modules specifically designed to meet various regulatory requirements, like data anonymization, consent management, or audit trails for HIPAA.*

Question: What kind of user training and support does the vendor provide?

Answer: *Expected answers include comprehensive documentation, training sessions, a dedicated support team, and possibly a certification program for users.*

Question: How are software updates and security patches managed?

Answer: *The vendor should have a predictable schedule for updates, emergency patch procedures, and a history of timely security updates.*

Question: What is the process for incident reporting and response within the software?

Answer: *There should be clear protocols for incident detection, containment, eradication, and recovery, along with post-incident analysis.*

Question: Does the software provide for separation of duties (SoD) to prevent fraud or errors?

Answer: *The system should enforce SoD through its access controls and transaction management to ensure no single individual has control over all aspects of any critical process.*

Question: Are there mechanisms for user behavior analytics (UBA) to detect anomalous behavior?

Answer: *The software should incorporate UBA to flag unusual activities that could indicate a security threat.*

Question: What is the vendor's policy on data ownership and data portability upon contract termination?

Answer: *Clear policies stating that data ownership remains with the client and provisions for secure, complete data extraction at the end of the contract should be in place.*

GRC Security Validation Guideline for Software Evaluation

Author: Timothy G. Majerus

@thetimmajerus

1. **Introduction:**

- Document Purpose: This document outlines the security validation process for evaluating new software to ensure it meets the [Company] GRC standards.
- Software Under Evaluation: [Software Name / Version]

2. **Scope:**

- In Scope:
  - Security features of the software.
  - Compliance with legal, regulatory, and corporate policies.
  - Risk assessment associated with software integration.
- Out of Scope:
  - Performance benchmarking not related to security.
  - User interface and experience unless related to security practices.

3. **Governance:**

- Standards and Regulations:
  - GDPR, HIPAA, ISO/IEC 27001, ADA etc., as applicable.
- Corporate Policies:
  - Data protection policies.
  - Access control policies.
  - Incident response plans.
- Roles and Responsibilities:
  - Security Team: Conduct the evaluation.
  - IT Department: Implement software securely if approved.
  - Compliance Officer: Ensure all regulatory requirements are met.

4. **Risk Management:**

- Risk Identification:
  - Vulnerability to known threats.
  - Potential for data breaches.
  - Integration risks with existing systems.

- **Risk Assessment:**
  - Likelihood of occurrence.
  - Impact on business operations, data integrity, and confidentiality.
- Risk Mitigation Strategies:
  - Proposed controls or software configurations to mitigate identified risks.

5. **Compliance:**
   - Checklist:
     - Data Privacy: Does the software handle data according to privacy laws?
     - Audit Trails: Capability to log access and changes.
     - Encryption: Use of encryption for data at rest and in transit.
     - Access Controls: Implementation of least privilege, separation of duty, 4and need-to-know principles.
   - Validation Tests:
     - Penetration testing results.
     - Static and dynamic code analysis.
     - Compliance with secure coding practices.
6. **Validation Process:**
   - Static Analysis: Review of software code for security vulnerabilities.
   - Dynamic Analysis: Testing the software in runtime environment.
   - User Access Testing: Ensure role-based access controls are functioning.
   - Data Handling: Verify secure data transmission, storage, and disposal.
7. **Documentation and Evidence:**
   - Test Results: Detailed reports from security testing tools.
   - Configuration Documents: Secure configuration guides provided by the vendor or developed internally.
   - Compliance Certificates: If any, from third-party auditors or the software vendor.
8. **Approval:**
   - Security Sign-off: Confirmation that the software has passed all security checks.
   - Management Approval: Final approval for deployment within the organization.

9. **Review and Update:**

- Periodic Review: Schedule for re-evaluation based on updates or changes in compliance requirements.
- Update Log: Record of any changes to this document or the software's compliance status.

Approval Section:

- Security Team Lead: ___________________________
- Compliance Officer: ___________________________
- IT Director: ___________________________
- Date: ________________