Overview:

1. **Introduction2**

• 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, 3and 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_