# Software Review Procedure Template

## Introduction

This document outlines the procedure for conducting software reviews within the organization, ensuring alignment with ISO 27001 standards. Software reviews are critical to maintaining information security and mitigating risks associated with software implementation and updates. This procedure supports compliance with ISO 27001.

## Purpose

The purpose of this procedure is to establish a standardized approach for reviewing software to identify vulnerabilities, ensure compliance with organizational policies, and maintain the security and integrity of information systems.

## Scope

This procedure applies to all software applications used within the organization, including proprietary, open-source, and third-party software. It is applicable to employees, contractors, and any other parties involved in software acquisition, development, or deployment.

## Policy Statement

1. All software must undergo a formal review process before deployment or significant updates. Significant updates include major version changes, critical security patches, or modifications that affect system functionality or integration.
2. Software reviews must assess compliance with organizational security requirements and applicable regulatory standards.
3. Identified vulnerabilities or non-compliance issues must be addressed before deployment.
4. The review process must include documentation of findings and actions taken.
5. Regular audits of software in production must be conducted to ensure ongoing compliance.

## Roles and Responsibilities

* Software Review Team: Conducts the review, identifies vulnerabilities, and ensures compliance.
* Information Security Officer: Oversees the software review process and approves the final deployment.
* System Owners: Provide necessary information about the software and implement recommended changes.
* Audit Team: Conducts periodic checks to verify the effectiveness of the software review process.

## Compliance and Monitoring

* Periodic internal audits to evaluate adherence to the review process, conducted quarterly.
* Documentation reviews to ensure completeness and accuracy, verified during each review cycle.
* Metrics tracking to assess the timeliness and effectiveness of reviews, including metrics such as average time to resolve vulnerabilities and percentage of reviews completed on schedule.
* Non-compliance incidents and corrective actions must be reported to senior management and logged for trend analysis.

## Related Documentation

* Information Security Policy
* Risk Management Framework
* Change Management Procedure
* ISO 27001 Standard

## Review and Revision

This procedure will be reviewed annually or in response to significant changes in technology, regulatory requirements, or organizational processes. The Information Security Officer will be responsible for initiating the review process. Updates will be approved by the Information Security Committee and communicated to all relevant stakeholders.

# Step-by-Step Software Review Process

## 1. Initiation

* Identify software for review and categorize it based on risk (e.g., high, medium, low).
* Notify stakeholders and schedule the review.
* Use a checklist template to ensure all required documentation is gathered, including software specifications, security requirements, vendor certifications, and previous audit reports.

## 2. Preliminary Assessment

* Conduct an initial risk assessment to identify potential security and compliance concerns.
* Review vendor certifications and third-party audit reports, if applicable.
* Determine the scope of the review based on identified risks.

## 3. Detailed Review

* Analyze the software code (if accessible) for vulnerabilities using automated tools (e.g., static code analysis).
* Assess software against organizational security policies, industry standards, and regulatory requirements (e.g., OWASP guidelines).
* Conduct functional and penetration testing using established methodologies to identify potential security gaps.
* Compile findings in a structured format for consistency.

## 4. Documentation and Reporting

* Document findings, including identified vulnerabilities and compliance gaps.
* Provide recommendations for mitigation and improvement.
* Share the review report with the Software Review Team and other relevant stakeholders.

## 5. Remediation

* Address identified vulnerabilities or compliance issues.
* Validate that corrective actions have been implemented effectively.
* Reassess the software to confirm resolution of issues.

## 6. Approval and Deployment

* Obtain final approval from the Information Security Officer.
* Document the approval and ensure all required records are maintained.
* Deploy the software in accordance with the Change Management Procedure.

## Narrative Guidance

The software review procedure aims to integrate security and compliance considerations seamlessly into the software lifecycle. By aligning with ISO 27001 principles, this process reduces risks associated with software vulnerabilities and enhances organizational resilience. Ensuring documentation, consistent monitoring, and periodic audits supports the goal of continuous improvement and regulatory adherence.