

KNOW WHERE YOUR SOFTWARE IS VULNERABLE. THE OUNCE COMPLIANCE GUIDE

The need for software security accountability is growing. No longer willing to race hackers to discovered vulnerabilities, organizations must now take a more proactive approach to the way they design, develop and operate the software on which their business relies. To enforce this, regulations have been developed in every industry to try to hold organizations accountable for insecure software and its resultant risk to customer data. Compliance frameworks providing guidance on how to implement these regulations, offer the necessary steps for ongoing, measurable software security assurance programs.

Businesses, armed with automated software security assurance tools such as those from Ounce Labs, can now have the metrics and policy compliance information they need to report to key executives, auditors and regulators on the process and state of their software security assurance efforts. This guide provides key personnel charged with fulfilling these various requirements with a quick reference to understanding:

- **The major compliance categories** into which software security assurance activities fall, including Risk Assessment, setting standards for Development and Deployment, and Vulnerability Identification and Remediation.
- **The applicable regulatory and compliance frameworks** and the specific control activities within each that apply to software security assurance activities.
- **The Ounce Labs solution** and the way in which its capabilities can provide the necessary metrics and policy compliance information to help prove compliance with these activities.

The regulatory and compliance frameworks covered in this guide include:

- **Sarbanes-Oxley:** Central to this regulation's mission is the need for reliable financial information from public companies. The ramifications of this requirement include enormous organizational shifts, and an attendant focus on the software and systems that house financial data. In creating IT control objectives to comply with Sarbanes-Oxley, organizations must assess risk, control relationships and deliverables from outsourcers, integrate security into the software development process, and monitor all changes that might impact critical systems.
- **CobIT:** As a compliance framework, CobIT provides a rigorous process of best practices for organizations, closely aligning IT with the business functions and specifically detailing software security assurance tasks for businesses to follow. CobIT assigns security activities to all aspects of the software process, from design and development, to risk assessment and security audit for software developed in- and out-of-house.
- **COSO:** A recognized formal model for compliance with Sarbanes-Oxley, the COSO framework establishes elements of internal control as interrelated components; central to each component is the need for software security assurance.
- **ISO17799:** Considered the major international standard for information security, ISO 17799 provides a comprehensive set of best practices and IT controls for organizations to follow. Software security assurance is central to its mission, requiring security compliance reviews and source code analyses as part of systems development and compliance management.

Until recently, focusing security assurance efforts on software was not a practical, achievable task. In the wake of these new regulations and compliance frameworks, however, a software assurance process must be incorporated into the organization. This quick reference guide should serve as a useful tool for understanding how a systematic approach to software security assurance including Ounce Labs can provide a single set of critical data and metrics to use for compliance, and how these activities map to broadly-applicable regulations and compliance frameworks.

	Software Security Assurance Controls	Pertinent Activities	COBIT	ISO 17799	COSO Component	IT Control Objectives for Sarbanes-Oxley (IT Governance Institute)	Ounce Labs Advantages
Risk Assessment	Assess level of risk: Identify, prioritize, and develop remediation strategy to mitigate or accept relevant software risks.	Prepare risk management plan to address most significant risks. Determine “risk appetite” and define acceptable levels of security risk. Consider cost-effective means to identify and manage the identified security risks through security practices. Develop risk management strategy to mitigate software risk and establish security controls.	AI1: 1.9 Cost-Effective Security Controls DS5: 5.8 Data Classification DS7: 7.3 Security Principles and Awareness Training PO9: 9.1 Business Risk Assessment 9.3 Risk Identification 9.5 Risk Action Plan	3.1 Establish an information security policy 4.1 Establish a security infrastructure 4.2 Coordinate information security implementation 5.2 Use an information classification system 6.3 Respond to information security incidents 10.1 Identify system security requirements	Risk Assessment	The IT organization’s risk assessment framework measures the impact of risks according to qualitative and quantitative criteria, using inputs from different areas including, but not limited to, management brainstorming, strategic planning, past audits and other assessments. The IT organization’s risk assessment framework is designed to support cost-effective controls to mitigate exposure to risks on a continuing basis, including risk avoidance, mitigation or acceptance.	Rapid cross-enterprise assessment: By automating the software analysis process, Ounce Labs allows organizations to rapidly assess the level of risk to their business posed by their applications.
Vulnerability Management and Remediation	Test software and technology infrastructure: Review acceptance criteria and evaluate code to determine acceptable security thresholds prior to deployment.	Test software against functional and operational system requirements, which should include business value and security threshold requirements.	AI5: 5.7 Testing of Changes 5.9 Final Acceptance Test 5.11 Operational Test 5.12 Promotion to Production 5.13 Evaluation of Meeting User Requirements, 5.14 Management’s Post-Implementation Review	4.1 Establish a security infrastructure 5.1 Make information asset owners accountable 8.2 Develop plans to provide future capacity (8.2.1 use acceptance criteria to test systems)	Control Activities	The organization has a system development life cycle methodology that considers security, availability and processing integrity requirements of the organization. Procedures exist to ensure that system software is installed and maintained in accordance with the organization’s requirements.	Precise vulnerability identification: Ounce Labs automatically identifies vulnerable areas within source code, using a vulnerability knowledgebase with tens of thousands of entries, identifying such critical vulnerabilities as: Buffer Overflows Cross-site Scripting Error Handling Problems Privilege Escalations SQL Injection Command Injection Race Conditions Insecure Network Communications Poor Logging Practices Improper Database Access Insecure Access Control Insecure Account/Session Management Insecure Cryptography Denial of Service Native/Dynamic Code Vulnerabilities
Set Standards for Development and Deployment	Include software security as an acceptance criteria in service level agreements: Define and manage service levels.	Ensure that management establishes security requirements and regularly reviews compliance of internal SLA’s. Determine security of the delivered code through code analysis. Include security thresholds as part of acceptance criteria in requirements documents.	AI1: 1.1 Definition of Information Requirements AI4: 4.1 Operational Requirements and Service Levels DS1: 1.2 Aspects of Service Level Agreements 1.5 Review of SLA’s and Contracts	6.1 Control your personnel recruitment process 10.5 Control development and support 12.2 Perform security compliance reviews (12.2.2 Carry out penetration tests to detect information security vulnerabilities)	Control Environment Control Activities Monitoring	N/A	Accountability: Ounce Labs assessment data can provide objective acceptance criteria for outsourced development, providing the means to confirm compliance with secure coding policies prior to acceptance. Reduced Costs: Assessing and addressing software security assurance throughout the lifecycle results in dramatically lower development, patch management and incident response costs.
	Manage third party services: Require evidence of security acceptance criteria.	Mitigate security and confidentiality risk from third party providers by defining source code security acceptance criteria in Service Level Agreements. Require objective evidence of compliance with security acceptance criteria.	DS2: 2.3 Third-Party Contracts 2.6 Continuity of Services 2.7 Security Relationships	4.3 Control outsourced information processing (4.3.1 use contracts to control outsourced services) 6.3 Respond to information security incidents (6.3.2 Report security threats and weaknesses) 8.1 Establish operational procedures 8.7 Control interorganizational exchanges 10.5 Control development and support (10.5.5 control outsourced software development)	Control Environment Risk Assessment Control Activities Monitoring	Procedures exist and are followed to ensure that a formal contract is defined and agreed to for all third party services before work is initiated, including definition of internal control requirements and acceptance of the organization’s policies and procedures. A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.	Accountability: Ounce Labs assessment data can provide objective acceptance criteria for outsourced development, providing the means to confirm compliance with secure coding policies prior to acceptance. Flexibility: The Ounce Labs solution can be installed in the configuration that meets deployment requirements, from a portable laptop for evaluating software at off-site locations, to workgroups and across the enterprise.
Monitor and Audit	Manage changes: Ensure continuing security and stability of software by enforcing a strict change management procedure that includes patches and updates, scheduled or emergency.	Evaluate all changes, including patches, to establish impact on the integrity, exposure or loss of sensitive data, availability of critical services, and validity of important transactions by analyzing source code prior to rollout.	AI5: 5.7 Testing of Changes AI6: 6.4 Emergency Changes	8.1 Establish operational procedures (8.1.2 Control changes to facilities and systems) 10.5 Control development and support (10.5.4 Inspect all source code before you use it)	Control Activities Monitoring	Procedures exist to ensure that system software changes are controlled in line with the organization’s change management procedures. IT management ensures that the setup and implementation of system software do not jeopardize the security of the data and programs being stored on the system.	Metrics-based reporting: Ounce Labs rates applications based on V-Density, providing an objective metric to evaluate delivered code against security acceptance criteria for internal teams or outsourced developers. Detailed software audit progress reports form the foundation of an ongoing vulnerability management program.
	Regularly evaluate the performance of information security. Review software for compliance with requirements and current security conditions.	Assess adequacy of defined security controls. Evaluate software for weaknesses.	M1: 1.2 Assessing Performance 1.3 Assessing Customer Satisfaction 1.4 Management Reporting M2: 2.1 Internal Control Monitoring	9.7 Monitor system access and use 12.2 Perform security compliance reviews	Control Activities Information and Communication Monitoring	The IT organization monitors is progress against the strategic plan and reacts accordingly to meet established objectives.	Audit reports: Ounce Labs offers a full range of audit reports, documenting and categorizing identified vulnerabilities and demonstrating improvements over time. Ongoing analysis: Whenever changes to these applications occur, Ounce Labs’ solutions rapidly and efficiently analyze software source code to enable detection of any new vulnerabilities that may have inadvertently been introduced.
	Software Audit: Obtain assurance of compliance with regulations and frameworks pertinent to critical systems, either through a third party or internal audit team.	Review security controls; assess compliance with laws, regulations and contracts.	M3: 3.3 Independent Effectiveness Evaluation of IT Services 3.4 Independent Effectiveness Evaluation of Third-Party Service Providers 3.5 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments 3.6 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third Party Service Providers 3.7 Competence of Independent Assurance Function	N/A	N/A	N/A	The organization monitors changes in external requirements for legal, regulatory or other external requirements related to IT practices and controls. Control activities are in place and followed to ensure compliance with external requirements, such as regulatory and legal rules.

OUNCE LABS: AUTOMATING SOFTWARE SECURITY ASSURANCE

The twin challenges of securing critical business data while complying with regulatory demands for security certification have created the urgent need to automate the process of software security assurance. Organizations need a practical, efficient, and measurable way to validate the security of critical systems, identify and prioritize remediation targets, and report on progress over time, for both new and legacy systems. These challenges demand a new solution.

Ounce Labs helps companies achieve software security assurance by identifying, measuring, and tracking vulnerabilities in source code. Ounce Labs' product suite analyzes software source code using patents-pending compiler-based source code analysis and providing tailored interactive vulnerability reports to security executives, managers and developers.

With Ounce Labs you can:

- **Improve security:** Identify and remove software vulnerabilities before they become a threat to your agency mission.
- **Reduce costs:** Eliminate software vulnerabilities prior to deployment for dramatic reductions in development, patch management, and incident response costs.
- **Prove compliance:** Certify that outsourcers meet your secure coding standards. Validate software meets acceptance criteria prior to deployment. Measure and document your software assurance program to meet your regulatory and internal software assurance audit reporting requirements.

PROVE PROGRESS

Ounce Labs' V-Density™ (vulnerability density) metric allows managers to evaluate delivered code against security acceptance criteria. By using V-Density to set an acceptable security threshold, these requirements can be built in to service level agreements, holding internal teams and outsourced development groups accountable for the security of delivered code.

With Ounce Labs, security executives can achieve reliable, actionable data to support Sarbanes-Oxley compliance efforts and adherence to IT audit frameworks by:

- Automatically identifying vulnerabilities within software
- Assessing software for implementation of required security mechanisms (i.e., encryption, access control, logging)
- Providing remediation advice for specific vulnerabilities to eliminate risk
- Tracking and reporting on improvements to application security over time

Ounce Labs offers a full range of audit reports, documenting and categorizing identified vulnerabilities and demonstrating improvements over time. These configurable progress reports may be provided to auditors and analysts to establish a baseline and continue to demonstrate system improvement over time.

LEADERSHIP IN SOFTWARE SECURITY ASSURANCE

With identity theft on the rise, and the costs of compliance and patch management skyrocketing, implementing and automating a software security assurance process is an important priority for organizations concerned with both security and effective controls. Complying with regulations such as Sarbanes-Oxley requires thorough analysis of the systems on which businesses rely, and the integration of security controls throughout the software lifecycle. With precise, consistent, actionable metrics, Ounce Labs provides executives with the necessary information to understand levels of software risk, identify next steps to remediate those threats, and demonstrate improvement over time. Precision, efficiency, and proof of progress in your software security assurance efforts: this is the Ounce Labs advantage.