

# KNOW WHERE YOUR SOFTWARE IS VULNERABLE.

## COMPLIANCE GUIDE FOR FINANCIAL SERVICES

Financial services organizations manage among the most critical and private data in the world, yet must make their systems open and available across the web. These competing requirements demand the highest levels of security assurance in the software that manages and transmits this critical data. Reflecting this concern, regulations and compliance frameworks have been created, holding organizations accountable for insecure software and its risk to customer data, and requiring ongoing, measurable software security assurance programs.

Businesses, armed with automated software security assurance tools such as Ounce Labs provides, 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:

- 1. The major compliance categories** into which software security assurance activities fall, including Risk Assessment and Vulnerability Management and Remediation.
- 2. The applicable regulatory and compliance frameworks** and the specific control activities within each that apply to software security assurance activities.
- 3. The Ounce Labs solution** and the way in which its capabilities 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:

- **GLBA and the FFIEC:** Gramm-Leach-Bliley Act section 501(b) describes the need for standards to safeguard financial customer information. The Federal Financial Institutions Examination Council's (FFIEC) Information Security IT Examination Handbook provides a rigorous security program designed to help financial institutions mitigate the risk presented by their applications and systems.
- **Payment Card Industry Data Security Standard (PCI):** In the wake of high-profile identity theft and fraud concerns, VISA and MasterCard are now requiring organizations that process cardholder data to comply with their PCI Data Security Standard. PCI details twelve key requirements designed to reduce the risk from the electronic transmission of cardholder data, and devotes substantial focus on the development and maintenance of secure systems and applications.
- **Sarbanes-Oxley:** This regulation's central mission is reliable financial information from public companies, requiring an attendant focus on the software and systems that house financial data. In creating IT controls for compliance, organizations must assess risk, control relationships and deliverables from outsourcers, integrate security into the development process, and monitor all changes that might impact critical systems.
- **CobIT:** As a compliance framework, Cobit provides a rigorous process, closely aligning IT with business processes and standards such as COSO, and specifically detailing software security assurance tasks for businesses to follow throughout the software development process.
- **ISO 17799:** 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 Assurance Requirements	Pertinent Activities	FFIEC Information Security IT Examination Handbook (GLBA)	Payment Card Industry Data Security Standard (PCI)	IT Control Objectives for Sarbanes-Oxley	COBIT	ISO/IEC 17799	Ounce Labs Advantages																		
Risk Assessment	<p><b>Assess level of risk:</b> Identify, prioritize, and develop remediation strategy to mitigate or accept relevant software risks</p>	<p>Prepare risk management plan to address most significant risks.</p> <p>Determine “risk appetite” and define acceptable levels of system security risk</p> <p>Consider cost-effective means to identify and manage the identified security risks through security practices</p> <p>Develop risk management strategy to mitigate software risk and establish security controls</p>	<p>A risk assessment provides a foundation for the remainder of the security process by guiding the selection and implementation of security controls and the timing and nature of testing those controls. Testing results, in turn, provide evidence to the risk assessment process that the controls selected and implemented are achieving their intended purpose. Testing can also validate the basis for accepting risks.</p> <p>Management may decide that since some risks do not meet the threshold set in their security requirement, they will accept those risks and not proceed with a mitigation strategy. Other risks may require immediate corrective action. Still others may require mitigation, either fully or partially, over time.</p>	<p>6.2 Establish a process to identify newly discovered vulnerabilities. Update your standards to address new vulnerability issues.</p>	<p>Management prepares strategic plans for IT that align business objectives with IT strategies.</p> <p>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.</p> <p>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.</p>	<p>PO9: 9.1 Business Risk Assessment 9.3 Risk Identification</p> <p>DS5: 5.8 Data Classification</p> <p>PO9: 9.5 Risk Action Plan</p> <p>AI1: 1.9 Cost-Effective Security Controls</p> <p>DS7: 7.3 Security Principles and Awareness Training</p>	<p>3.1 Establish an information security policy</p> <p>4.1 Establish a security infrastructure</p> <p>4.2 Coordinate information security implementation</p> <p>5.2 Use an information classification system</p> <p>6.3 Respond to information security incidents</p> <p>10.1 Identify system security requirements</p>	<p><b>Rapid cross-enterprise assessment:</b> By automating the software analysis process, Ounce Labs allows organizations to rapidly assess the level of risk posed to their business by their applications.</p>																		
Vulnerability Management and Remediation	<p><b>Test software and technology infrastructure:</b> Review acceptance criteria and evaluate code to determine acceptable security thresholds prior to deployment</p>	<p>Test software against functional and operational system requirements, which should include business value and security threshold requirements.</p>	<p>Application and operating system source code can have numerous vulnerabilities due to programming errors or misconfiguration. Where possible, financial institutions should use software that has been subjected to independent security reviews of the source code, especially for Internet facing systems.</p>	<p>6.3 Develop software application based on industry best practices and include information security throughout the software development lifecycle.</p> <p>6.3.7 Review of custom code prior to release to production or customers to identify any potential coding vulnerability.</p> <p>6.5 Develop web software and applications based on secure coding guidelines such as the Open Web Application Security Project (OWASP) guidelines. Review custom application code to identify coding vulnerabilities.</p>	<p>The organization has a system development life cycle methodology that considers security, availability and processing integrity requirements of the organization.</p> <p>Procedures exist to ensure that system software is installed and maintained in accordance with the organization’s requirements.</p>	<p>AI5: 5.7 Testing of Changes 5.11 Operational Test 5.12 Promotion to Production</p> <p>AI5: 5.9 Final Acceptance Test 5.13 Evaluation of Meeting User Requirements 5.14 Management’s Post-Implementation Review</p>	<p>4.1 Establish a security infrastructure</p> <p>5.1 Make information asset owners accountable</p> <p>8.2 Develop plans to provide future capacity (8.2.1 Use acceptance criteria to test systems)</p>	<p><b>Precise vulnerability identification:</b> Ounce Labs automatically identifies vulnerable areas within source code, using a vulnerability knowledgebase with tens of thousands of entries, identifying critical vulnerabilities as defined by the OWASP and others as:</p> <table border="0"> <tr> <td>Buffer Overflows</td> <td>Insecure Account/Session Management</td> </tr> <tr> <td>Insecure Network Communications</td> <td>Command Injection</td> </tr> <tr> <td>Cross-site scripting</td> <td>Insecure Cryptography</td> </tr> <tr> <td>Poor Logging Practices</td> <td>Race Conditions</td> </tr> <tr> <td>Error Handling Problems</td> <td>Denial of Service</td> </tr> <tr> <td>Improper Database Access</td> <td>Insecure Network Communications</td> </tr> <tr> <td>Privilege Escalations</td> <td>Native/Dynamic Code Vulnerabilities</td> </tr> <tr> <td>Insecure Access Control</td> <td></td> </tr> <tr> <td>SQL Injection</td> <td></td> </tr> </table>	Buffer Overflows	Insecure Account/Session Management	Insecure Network Communications	Command Injection	Cross-site scripting	Insecure Cryptography	Poor Logging Practices	Race Conditions	Error Handling Problems	Denial of Service	Improper Database Access	Insecure Network Communications	Privilege Escalations	Native/Dynamic Code Vulnerabilities	Insecure Access Control		SQL Injection	
Buffer Overflows	Insecure Account/Session Management																									
Insecure Network Communications	Command Injection																									
Cross-site scripting	Insecure Cryptography																									
Poor Logging Practices	Race Conditions																									
Error Handling Problems	Denial of Service																									
Improper Database Access	Insecure Network Communications																									
Privilege Escalations	Native/Dynamic Code Vulnerabilities																									
Insecure Access Control																										
SQL Injection																										
Set Standards for Development and Deployment	<p><b>Include software security as an acceptance criteria in service level agreements with third parties:</b> Define and manage service levels.</p>	<p>Ensure that management establishes security requirements and regularly reviews compliance of internal SLAs and contracts with 3rd party service providers.</p>	<p>Establish security requirements, acceptance criterion and test plans</p> <p>Review and test source code for security vulnerabilities, including covert channels or backdoors that might obscure unauthorized access into the system.</p> <p>Perform security tests to verify that the security requirements are met before implementing the software in production.</p>	<p>Contractually require all third parties with access to cardholder data to adhere to payment card industry security requirements.</p> <p>12.4 Ensure the security policy and procedures clearly define information security responsibilities for all employees and contractors.</p> <p>12.8.1 Acknowledgement that the 3rd party is responsible for the security of cardholder data in their possession.</p>	<p>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.</p> <p>A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.</p>	<p>DS1: 1.2 Aspects of Service Level Agreements 1.5 Review of SLAs and Contracts</p> <p>DS2: 2.3 Third-Party Contracts 2.7 Security Relationships 2.8 Monitoring</p> <p>AI4: 4.1 Operational Requirements and Service Levels</p>	<p>4.3 Control outsourced information processing (4.3.1 Use contracts to control outsourced services)</p> <p>6.3 Respond to information security incidents (6.3.2 Report security threats and weaknesses)</p> <p>8.1 Establish operational procedures</p> <p>8.7 Control interorganizational exchanges</p> <p>10.5 Control development and support (10.5.5 Control outsourced software development)</p> <p>12.2 Perform security compliance reviews (12.2.2 Carry out penetration tests to detect information security vulnerabilities)</p>	<p><b>Accountability:</b> 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.</p> <p><b>Reduced Costs:</b> Assessing and addressing software security assurance throughout the lifecycle results in dramatically lower development, patch management and incident response costs.</p> <p><b>Flexibility:</b> 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.</p>																		
Monitor and Audit	<p><b>Manage changes:</b> Ensure continuing security and stability of software by enforcing a strict change management procedure that includes patches and updates, scheduled or emergency.</p>	<p>Evaluate all changes, including patches, to establish the 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.</p>	<p>The source code reviews should be repeated after the creation of potentially significant changes.</p>	<p>11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.</p>	<p>[Expect] risk assessments built into the program change process.</p> <p>Procedures exist to ensure that system software changes are controlled in line with the organization’s change management procedures.</p> <p>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.</p>	<p>AI5: 5.7 Testing of changes</p> <p>AI6: 6.4 Emergency Changes</p>	<p>8.1 Establish operational procedures (8.1.2 Control changes to facilities and systems.)</p> <p>10.5 Control development and support (10.5.4 Inspect all source code before you use it)</p>	<p><b>Metrics-based reporting:</b> 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 team.</p> <p><b>Ongoing analysis:</b> 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.</p>																		
	<p><b>Regularly audit and evaluate the performance of information security.</b> Review software for compliance with requirements, regulations and frameworks pertinent to critical systems, either through a third party or internal audit team.</p>	<p>Assess adequacy of defined security controls.</p> <p>Evaluate software for weaknesses.</p> <p>Review security controls; assess compliance with laws, regulations and contracts.</p>	<p>Risk assessments should be updated as new information affecting information security risks are identified. At least once a year, senior management should review the entire risk assessment to ensure relevant information is appropriately considered.</p> <p>Institutions should design tests to produce results that are logical and objective. Results that are reduced to metrics are potentially more precise and less subject to confusion, as well as being more readily tracked over time.</p>	<p>11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.</p>	<p>The IT organization monitors its progress against the strategic plan and reacts accordingly to meet established objectives.</p> <p>The organization monitors changes in external requirements for legal, regulatory or other external requirements related to IT practices and controls.</p> <p>Control activities are in place and followed to ensure compliance with external requirements, such as regulatory and legal rules.</p>	<p>M1: 1.2 Assessing Performance 1.3 Assessing Customer Satisfaction 1.4 Management Reporting</p> <p>M2: 2.1 Internal Control Monitoring</p> <p>M3: 3.4 Independent Effectiveness Evaluation of Third-Party Service Providers</p> <p>3.5 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments.</p> <p>3.6 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third Party Service Providers.</p>	<p>9.7 Monitor system access and use</p> <p>12.2 Perform security compliance reviews</p>	<p><b>Audit Reports:</b> Ounce Labs offers a full range of audit reports, documenting and categorizing identified vulnerabilities and demonstrating improvements over time.</p> <p><b>Cross-lifecycle Assessments:</b> Because Ounce Labs can be deployed at the earliest point in the lifecycle, measurable, tangible proof of both process and progress can be provided from the onset of coding through the maintenance and upgrade phases of any project. This automated approach ensures that software security assurance is ‘baked in’, rather than added on, helping deliver secure applications.</p>																		

## 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. Financial institutions 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, including coding errors, design flaws, and policy violations. Ounce Labs' product suite analyzes software source code using patents-pending compiler-based analysis and provides tailored interactive vulnerability reports to security executives, managers and developers. With Ounce Labs you can:

- **Assess Your Software:** Rapidly and accurately analyze your software for coding errors, design flaws, and policy violations.
- **Understand Your Exposure:** Prioritize, address, and report on software risk, across your software portfolio.
- **Manage Your Enterprise-Wide Risk:** Ounce delivers a solution with the most reliable, scalable, robust technology in the industry to help you manage your risk enterprise-wide.

## 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 and GLBA 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 GLBA and Sarbanes-Oxley requires thorough analysis of the systems on which financial organizations 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.