

KNOW WHERE YOUR SOFTWARE IS VULNERABLE.

COMPLIANCE GUIDE FOR FEDERAL AGENCIES

Increasingly, US federal agencies rely on complex and internetworked software to enable their mission. As federal services from taxpayer information to national defense move onto the Web, agencies have a driving need to ensure that the software managing those services and related data is written securely. The regulatory environment has expanded recently to address the need for ongoing, measurable software security assurance programs, and is mandating that agencies demonstrate their compliance.

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

- 1. The major compliance categories** into which software security assurance activities fall, including Risk Assessment, Identification and Authentication, and Vulnerability 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 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:

- **FISMA:** This core federal security mandates software security assurance calls for “periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.”¹ Key implementation guide: NIST’s Special Publication 800 Series
- **DITSCAP/DIACAP:** Applying specifically to the National Security Agency and the Department of Defense (DoD), these regulations require its agencies to “evaluate security vulnerabilities with regard to confidentiality, integrity, availability and accountability and recommend applicable countermeasures... [the systems must be] analyzed to determine its susceptibility to exploitation, the potential rewards to the exploiter, the probability of occurrence, and any related threat.”² *Key Implementation Guide: Defense Information Systems Agency’s (DISA) Application Security Checklist*

This guide also provides alignment with the DoD’s Instruction #8500.2, Information Assurance Implementation, and ISO 17799. Implementing these control activities, specifically with financial systems, will significantly advance agency efforts to comply with the OMB Circular A-123, or “Sarbanes-Oxley for the Fed”, which will become a requirement in fiscal year 2006.

As many agencies are responsible for reporting across various regulatory and compliance frameworks, 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 reporting across multiple frameworks.

OUNCE LABS: AUTOMATING SOFTWARE SECURITY ASSURANCE

The twin challenges of securing our national software infrastructure while complying with regulatory demands for security certification have created the urgent need to automate the process of software security assurance. Agencies 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.

Compliance Category	NIST Special Publication 800-53 (NIST Implementation Guide for FISMA)	Department of Defense Instruction #8500.2, Information Assurance Implementation	DISA Application Security Checklist	ISO 17799	Ounce Labs Advantages															
Identification and Authentication	IA-7 Cryptographic Module Authentication SC-13 Use of Validated Cryptography	IAKM-1 Key Management IATS-1 Token and Certificate Standards DCNR-1 Non repudiation ECCR-1 Encryption for Confidentiality (Data at Rest) ECCR-2 Encryption for Confidentiality (Data at Rest) (classified non-SAMI)	APP0140 An application user or client authentication process is inadequate (must inventory all client authentication processes in the application) APP0330 The application utilizes an unapproved cryptographic module APP0580 Application users can circumvent the intended user interface to access resources in its supporting infrastructure.	9.1 Control access to information 10.3 Use cryptography to protect information 10.3.1 Develop a policy on the use of cryptography	Automated analysis: Ounce Labs automatically identifies vulnerable areas within source code, including insecure access controls and insecure cryptography. By rapidly identifying these areas, agencies may more efficiently and effectively determine and report their findings. Audit reports: Ounce Labs offers a full range of audit reports, documenting and categorizing identified vulnerabilities and demonstrating improvements over time.															
Risk Assessment	RA-3 Risk Assessment: Conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Risk assessment take into account vulnerabilities, threat sources, and security controls. RA-4 Risk Assessment Update: Update the risk assessment whenever there are significant changes to the information system, facility, or other conditions	DCDS-1 Dedicated IA Services DCII-1 Impact Assessment E3.3.10 DoD IA program shall regularly and systematically assess information systems, services and supporting infrastructures	N/A	4.0, Organizational Security 4.1 Establish a security infrastructure 4.2 Control third party access to facilities 6.2.1 Control your information security training	Rapid cross-enterprise assessment: By automating the software analysis process, Ounce Labs allows agencies to rapidly assess the level of risk to their organization posed by their applications. 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.															
Vulnerability Management	RA-5 Vulnerability Scanning: Using appropriate vulnerability scanning tools and techniques, scan for vulnerabilities in the information system or when significant new vulnerabilities are identified and reported.	ECMT-1 Conformance Monitoring and Testing VIVM-1 Vulnerability Management	APP1020 The application does not adequately validate user inputs before processing them APP1030 The application is vulnerable to buffer overflows	8.2.2 Use acceptance criteria to test systems 8.3 Protect against malicious software 10.2.1 Build input data validation into your systems 10.2.4 Build output data validation into your systems 10.5.4 Safeguard against covert channels and Trojans (inspect all source code before you use it)	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: <table border="0"> <tr> <td>Buffer Overflows</td> <td>Cross-site Scripting</td> <td>Error Handling Problems</td> </tr> <tr> <td>Privilege Escalations</td> <td>SQL Injection</td> <td>Insecure Network Communications</td> </tr> <tr> <td>Race Conditions</td> <td>Command Injection</td> <td>Poor Logging Practices</td> </tr> <tr> <td>Improper Database Access</td> <td>Insecure Access Control</td> <td>Insecure Account/Session Management</td> </tr> <tr> <td>Insecure Cryptography</td> <td>Denial of Service</td> <td>Native/Dynamic Code Vulnerabilities</td> </tr> </table> 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.	Buffer Overflows	Cross-site Scripting	Error Handling Problems	Privilege Escalations	SQL Injection	Insecure Network Communications	Race Conditions	Command Injection	Poor Logging Practices	Improper Database Access	Insecure Access Control	Insecure Account/Session Management	Insecure Cryptography	Denial of Service	Native/Dynamic Code Vulnerabilities
Buffer Overflows	Cross-site Scripting	Error Handling Problems																		
Privilege Escalations	SQL Injection	Insecure Network Communications																		
Race Conditions	Command Injection	Poor Logging Practices																		
Improper Database Access	Insecure Access Control	Insecure Account/Session Management																		
Insecure Cryptography	Denial of Service	Native/Dynamic Code Vulnerabilities																		
Outsourced Information System Services	SA-9 Outsourced Information System Services: Third party providers employ adequate security controls, and the organization monitors security control compliance. Third party providers are subject to the same information system security policies and procedures of the organization. Service level agreements define the expectations of performance, describe measurable outcomes, and identify remedies for non-compliance.	DCDS-1 Dedicated IA Services DCIT-1 IA for IT Services	N/A	10.5.4 Safeguard against covert channels and Trojans (inspect all source code before you use it) 10.5.5 Control outsourced software development	Accountability: Ounce Labs assessment data can provide objective acceptance criteria for outsourced development, providing the means to confirm compliance with agency 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 agency-wide.															
Security Testing	SA-11 Developer Security Testing: Developer creates a security test and evaluation plan, implements the plan and documents results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system. SA-3 Life Cycle Support: The organization manages the information system using a system development lifecycle methodology that includes information security considerations.	E3.4.4 All applications shall employ Information System Security Engineering (ISSE) as part of acquisition process or development to ensure IA is built in 5.8.1 Ensure that IA is incorporated as an element of DoD information system life cycle management processes	N/A	12.2 Perform security compliance reviews 12.2.2 Review technical security compliance (carry out penetration tests to detect information security vulnerabilities)	Cross-lifecycle Assessments: 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 assurance is 'baked in', rather than added on, helping deliver applications secure enough to support the agency's mission. Reduced Costs: Assessing and addressing software security assurance throughout the lifecycle results in dramatically lower development, patch management and incident response costs.															
Vulnerability Remediation	SI-2 Flaw Remediation: The organization identifies, reports, and corrects system flaws. The organization identifies information systems containing proprietary or open source software affected by recently announced software flaws. Flaws discovered during security assessments should also be addressed.	DCSQ-1 Software Quality DCCT-1 Compliance Testing	APP1020 The application does not adequately validate user inputs before processing them APP1030 The application is vulnerable to buffer overflows	10.2.1 Build input data validation into your systems 10.2.4 Build output data validation into your systems 10.5.4 Safeguard against covert channels and Trojans (inspect all source code before you use it)	Line-by-line remediation advice: Ounce Labs provides in-context remediation advice for each vulnerability, for straightforward elimination of vulnerabilities and on-the-job training in secure coding best practices. Detailed audit reporting: Ounce Labs reporting documents the process and progress of vulnerability remediation efforts for auditors, regulators, and program management.															

Ounce Labs helps agencies 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 intra-agency software assurance 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 FISMA and DITSCAP/DIACAP compliance efforts 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

Software powers the nation's critical infrastructure, and therefore must be the central starting point for risk assessment and regulatory compliance. Complying with regulations such as FISMA and DITSCAP/DIACAP requires thorough analysis of the systems on which government agencies run. With precise, consistent, actionable metrics, Ounce Labs provides agency heads with the necessary information to understand their 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.

1. Federal Information Security Management Act of 2002, Public Law No. 107-347, December 17, 2002
2. Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), number 5200.40, December 30, 1997