SOLUTION FACT SHEET

Highlights

Independent Expert Review: Veracode is a recognized application security expert with experience in FISMA guidelines

Rapid Results: Perform analysis and receive results within 24 hours

Rapid Time to Compliance: Provides actionable advice for faster remediation by developers

Automated & Integrated: Automated application penetration testing with seamless integration into software development lifecycle

Streamline Costs: Subscription model provides consistent testing costs regardless of application testing frequency

Automated Risk Ranking: Assigns risk severity rankings based on CWE & CVSS to meet auditing standards

Training: Several online courses fulfill FISMA training program requirements

Benchmarking: Compare your state of FISMA compliance against that of peers

Secure Software Supply Chain: Understand and reduce the security risks associated with the use of vendor-supplied software

Continuous Monitoring: Analytics provides insight on all applications no matter where they reside

FISMA Compliance Simplified

An on-going application security program is a cornerstone of FISMA compliance. Veracode's approach to application security is the simplest approach to FISMA compliance.

The Federal Information Security Management Act (FISMA) holds agencies accountable for the secure handling of information. FISMA is based on a framework of guidance and controls maintained by the National Institute of Standards and Testing (NIST). In addition to the risk and potentially significant costs of information breaches themselves, non-compliance with FISMA can result in administrative sanctions and reduced agency budgets.

Those subject to FISMA regulations include not only government agencies, but any organization that manages or provides information systems. The regulations also apply to organizations that exchange information with agency systems, including contractors and third party clearinghouses or vendors. Organizational responsibility for FISMA compliance may fall upon chief information/technology officers, information security officers, inspector generals, and agency program officials.

FISMA Aims for Security Assurance

NIST SP 800-53 Revision 4 introduces new and enhanced controls for increasing information system security assurance. The theme: "Build it Right – Continuously Monitor". The new controls focus on improving the security quality of technology/software as it is being built or acquired, and using a variety of testing techniques to provide agencies with assurance that the technology remains secure throughout its lifecycle.

There are significant changes in the System and Services Acquisition (SA) family of controls, and new and enhanced controls can also be found in System and Information Integrity (SI), Security Assessment and Authorization (CA) and Awareness and Training (AT).

Veracode's Platform Addresses New & Enhanced Controls

Veracode's Software as a Service (SaaS) application security testing platform helps agencies rapidly achieve FISMA compliance. The Veracode platform allows agencies to realize greater security assurance in a cost effective, easy to use, and simple to deploy manner.

For the first time, static and dynamic application security testing are specified in some of the new controls; Veracode's Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) provide a ready-made solution for many of these new testing requirements. In fact, static code analysis such as that performed by Veracode or a number of other tools is highlighted in the newly signed Department of Defense National Defense Authorization Act (NDAA) of 2013.

How Veracode Helps Agencies Achieve FISMA Compliance

Veracode has extensive experience partnering with federal departments and agencies to help them meet their regulatory requirements. Veracode provides full end-to-end security solutions and services for government agencies and subcontractors to help them meet FISMA compliance. Here is a sampling of Security Controls from NIST SP 800-53 Revision 4 and details on how Veracode can help.

System and Services Acquisition - Security Assurance for the Software Supply Chain

Veracode helps you manage risk across your entire application portfolio—in-house, outsourced, mobile, commercial-off-the-shelf (COTS), government-off-the-shelf (GOTS), and open-source applications.

Veracode's unique Vendor Application Security Testing program (VAST) is the only complete, independent solution designed to cost-effectively meet the new controls for the extended, more complicated software supply chain. As an independent third party, Veracode can broker the relationship for testing vendor-supplied software applications. VAST is currently being evaluated by the Department of Homeland Security as part of its Software Assurance Forum.

System and Services Acquisition - System Development Life Cycle

Veracode enables agencies to embed automated application security controls into their software development lifecycle (SDLC), software change management, and third-party software acquisition processes. With these automated controls, agencies can cost-effectively manage application security risk and sustain FISMA compliance.

Awareness and Training - Security Training

Veracode delivers secure training content in a web-based training format. Our training program is designed specifically for developers and security personnel to meet formal training and competency testing requirements. Courses can be taken at the user's own pace and the platform provides usage metrics, such as courses completed.

System and Information Integrity - Malicious Code Protection

Veracode has the ability to detect applications for Malicious Code threats that include Time Bombs, Hardcoded Cryptographic Constants and Credentials, Deliberate Information and Data Leakage, Rootkits and Anti-Debugging techniques. These targeted Malicious Code threats are hidden in software and mask their presence to evade detection by traditional security technologies. Veracode's detection capabilities provide the most comprehensive support to combat against backdoors and Malicious Code available in the market.

Security Assessment and Authorization - Continuous Monitoring

More controls are targeting continuous monitoring; the goal is to move away from one-off security audits of select functions or features, toward continuous diagnostics and remediation. Veracode's Application Perimeter Monitoring (APM) provides cost-effective continuous diagnostics on all your applications, no matter where they reside.

The Veracode Platform can be employed to regularly and automatically scan applications outside the direct control of IT. Such automated application testing can act as an extension of IT for agency security policy enforcement. APM can also include Manual Penetration Testing (MPT) for targeted sites or select functions, providing the desired level of due-diligence for cost-effective security assurance.

Learn More

Webinar: View the "Budgeting for Defense" webinar https://info.veracode.com/Budgeting-for-Defense-Registration.html

Solutions for Government: http://www.veracode.com/services/solutions-for-government.html

Contact Us: https://info.veracode.com/WebContactUs.html

Federal Contact: Justin DuHaime jduhaime@Veracode.com Office: (202) 903-0088 Cell: (703) 963-6270

VERACODE
Securing the Software That Runs the World

Veracode, Inc.
65 Network Drive
Burlington, MA 01803

Tel +1.339.674.2500
www.veracode.com