VERACODE

Compliance

Streamline compliance with industry regulations

DID YOU KNOW?

- ✔ 3 out of 5 applications assessed by Veracode fail the OWASP Top 10 and therefore would fail to comply with most compliance standards.
- ✔ Veracode worked with a large financial services firm to assess 38 applications that were in-scope for PCI. Initial assessments were completed within 30 days and all 38 were compliant with PCI 6.5 within 90 days.
- ✔ According to a Ponemon Institute study, industries subject to compliance requirements such as Healthcare, Education, Pharma and Financial Services have a per capita breach cost between 40% and 150% greater than the average.

Automation. Centralization. Comprehensive Controls.

To address growing concern over data breaches, various industries have issued regulations addressing cybersecurity and information security controls. In addition, enterprises in many industries are now holding their software vendors accountable for meeting standard application security policies. The challenge is that meeting these standards with manual processes and penetration testing is arduous, and most organizations can't address this challenge on their own because of lack of time, staff and money. Most end up merely "checking the box" and demonstrating compliance via minimal process documentation. As a result, these organizations and their suppliers are at risk of noncompliance, and worse, of breach.

Veracode enables you to address compliance requirements related to application security and secure development without having to manage tools or hire additional staff. The Veracode Application Security Platform provides access to a wide variety of methods to assess application security, along with compliance and development team reporting and secure development training. In addition, Veracode services help enterprises develop their cybersecurity strategy and deliver risk reduction results.

Track flaws, reviews and compliance through a single platform.

All Veracode services are delivered through the Veracode Application Security Platform, which provides a central repository for information about your software weaknesses, as well as proposed, accepted and rejected mitigations. And the same workflow can be used for static, dynamic or manual findings. With this central location, Veracode application security consultants can make more informed decisions on whether a proposed mitigation is effective because they can see the exact application data flow that was analyzed as part of the static analysis.

Achieve continuous compliance monitoring.

Best-practice organizations understand that to achieve the risk-reduction goals of mandated compliance standards, they cannot treat compliance as an end in itself but as the outcome of an ongoing process. Veracode helps deliver continuous compliance by providing application security testing that integrates into your software development lifecycle; conducting regular discovery scans of the web applications in your domain, including temporary marketing sites, international domains and sites obtained via M&A; continuously monitoring your production web applications for vulnerabilities; and providing virtual patching for your web application firewalls based on the security intelligence from your application assessments.

Detect and prevent web-based attacks.

With Veracode Runtime Protection, you add the option to instantly mitigate certain vulnerabilities without involving developers, so you're increasing development speed while managing your risk. Veracode Runtime Protection helps companies meet mandated standards by providing an automated solution that detects and prevents web-based attacks.

VERACODE

Educate developers in secure coding practices.

Compliance standards for developing secure code don't stop at testing software; many also recommend training developers in secure coding practices. Veracode Developer Training provides a variety of educational approaches to fit your team's needs, from on-demand computer-based training courses to remediation-focused AppSec tutorials and instructor-led deep dives on specific topics.

Automate and audit compliance workflows.

The Veracode Platform provides built-in, automated compliance workflows. These workflows reduce communication overhead and provide a secure audit trail of your compliance processes, including notifications about policy changes and approval workflows for mitigating controls that take a vulnerability out of scope for remediation. And the Policy Manager helps to document and communicate your security policy. When it's time to show compliance to auditors, you can share compliance status with EMC/RSA Archer via our native integration. Similar integrations are available for other GRC systems such as IBM OpenPages, RSAM, RiskVision, LockPath, Allgress and Symantec Control and Compliance Suite (CCS).

Compliance Standards Matrix

STANDARD	SECTIONS/CONTROLS SUPPORTED
PCI-DSS	6.1, 6.5, 6.6, 6.7, 11.3, 12.6
PA-DSS	5.1.7, 5.2, 7.1
HIPAA/HITRUST CSF	01.v, 02.e, 04.a, 06.d, 10.a, 10.b, 10.c, 10.l, 10.m
NIST 800-37	Tasks 1, 4, 5, 8, 9, 10
NIST 800-53	AT-2, 3, 4; CA-2, 7, 8; CM-4, 8; RA-2, 3, 5; SA-3, 4, 11, 12; SC-13; SI-2, 7, 10, 11, 12; PM-1, 6, 14
NIST 800-161	Controls for 800-53, plus AU-10; CM-7, 8; CP-2; PV-1, 2; RA-1; SA-8, 11, 12
New York Department of Financial Services Cybersecurity Regulations	500.05(a) 1,2; 500.06(a)2; 500.08(a); 500.11; 500.14(a)2
Monetary Authority of Singapore Technology Risk Management Guidelines	5, 6, 9.4, 12.2
Sarbanes-Oxley	Fraud prevention; protection of audit trails
OCC Bulletin 2013-29	Requires regulated entities to assess and manage risks associated with their third-party relationships
Securities and Exchange Commission Requirements for Cybersecurity	SEC has published guidance for public companies related to the disclosure of cybersecurity risks and the financial impact of cyber incidents such as data breaches. We can help by providing detailed analytics about the current risk profile for your application infrastructure as well as an assessment of the remediation work required after a successful application-layer attack.
FS-ISAC Third Party Software Controls	Control Type 2, 3a, 3b
GDPR	Articles 5, 24, 25, 28, 32, 33, 35

The Veracode Application Security Platform

Veracode enables you to comply with mandatory application security and secure development requirements without having to manage tools or hire additional staff.

WWW.VERACODE.COM