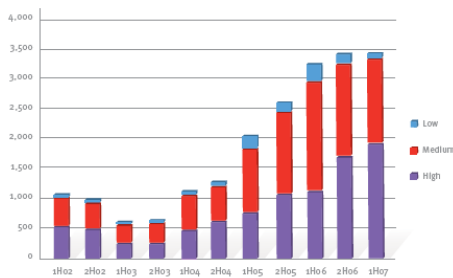


## Highlights

- **Rapid Time to SOX Compliance** – Receive reports and results within 24-72 hours
- **Automated & On-Demand** – Application security testing on an as-needed basis
- **Lower Compliance Costs** – Software as a Service (SaaS) means no hardware or software to purchase, install & maintain
- **Independent Expert Review** – Veracode is a recognized application security expert meeting compliance guidelines
- **Standards-Based Ratings** – Ratings based on NIST, CWE & CVSS to meet auditing standards

## Key Facts

- **Section 302** – Requires the CEO and CFO to quarterly certify the existence of internal controls and sign off on the veracity of the company's financial statements.
- **Section 404** – Requires annual evaluation and documentation of the internal controls and procedures in place to secure the integrity of financial information.
- **COBIT Framework** – Many organizations use the IT Governance Institute's COBIT framework to implement SOX compliant IT processes.
- **State of Software** – The National Vulnerability Database lists over 3,400 hundred vulnerabilities disclosed in the 1<sup>st</sup> half of 2007 alone



Software Vulnerability Disclosures (Source: NVD & Microsoft)

## Veracode Solutions for SOX

The Sarbanes–Oxley Act of 2002, or SOX, is a United States federal law passed in response to a number of major corporate and accounting scandals. The legislation is wide ranging and establishes new or enhanced standards for all U.S. public companies which are overseen by the newly created Public Company Accounting Oversight Board (PCAOB) in accordance with SEC rules. Businesses are required to have internal controls and procedures in place to secure the integrity of financial information in order to achieve SOX compliance.

Applications control financial transactions making security testing of these applications a critical component of SOX Section 404. To simplify SOX compliance, many companies use the IT Governance Institute's COBIT framework which is an exhaustive set of controls and can be used to assess compliance with SOX. Veracode's on-demand application security testing service allows public companies to embed application security testing into their COBIT processes as an automated control to cost-effectively achieve SOX compliance.

### Achieve SOX Compliance with SecurityReview

Veracode's SecurityReview helps public companies rapidly achieve SOX compliance in a simple and cost-effective way. Veracode's automated on-demand service allows organizations to conduct application security testing on an as-needed basis and without the need for costly tools or time intensive consultative engagements. Also, with no hardware or software to buy, install, maintain or upgrade companies can dramatically reduce both their capital and operational expenses related to SOX compliance. Organizations simply enter application information through Veracode's secure online portal and receive reports and results within 24-72 hours.

### Independent Review with Standards-Based Ratings

Auditors require proof that your applications are free from vulnerabilities and they need a method to evaluate findings against a well-known industry benchmark. Veracode's Ratings System solves this issue by producing a software security rating based on respected industry standards including NIST for definitions of assurance levels, MITRE's Common Weakness Enumeration (CWE) for classification of software weaknesses and FIRST's Common Vulnerability Scoring System (CVSS) for severity and ease of exploitability. These universally accepted vulnerability scoring methods provide auditors confidence that you have effective security controls in place.

*"Businesses should urge all IT vendors to use CVSS in their vulnerability and patch reporting."*

John Pescatore

Gartner



## Speed Remediation



Veracode's Fix First Analysis quickly identifies flaws to reduce the time & effort associated with SOX compliance



Veracode's On-Demand Service tracks your application's ratings over time, enabling you to create a plan of action with compliance project milestones

## Veracode Solutions for SOX Compliance

COBIT 4.1 Framework for SOX Compliance	Veracode Solution
AI2 Acquire and Maintain Application Software	<b>Vulnerability Assessments</b> - Veracode enables organizations to identify risks and address application security requirements as part of the software lifecycle process.
AI5 Procure IT Resources	<b>Vendor SecurityReview</b> - Veracode is the only solutions provider which can scan COTS applications without requiring access to source code, allowing companies to embed security into their procurement process in accordance with the COBIT framework.
AI7 Install and Accredit Solutions and Changes	<b>Independent Verification</b> - Veracode enables organizations to quickly conduct testing of changes and satisfy "independence" guidelines by providing an independent review and rating.
DS2 Manage 3rd Party Services	<b>Vulnerability Scanning</b> - Software used by suppliers to deliver critical services can be scanned to manage risks associated with vulnerabilities that may impact the integrity of financial reporting.
DS5 Ensure System Security	<b>Embed Security Management</b> - Veracode's SecurityReview is used to meet the COBIT framework security testing and malicious software prevention requirements.
PO9 Assess and Manage IT Risk	<b>Malicious Code and Backdoor Protection</b> - Veracode application testing allows organizations to assess risks and vulnerabilities in software that handles financial transactions.

## For More Information

For information on software security services, best practices, and methodologies, contact us at.

Veracode, Inc.  
 4 Van de Graaff Drive  
 Burlington, MA 01803  
 Phone: +1.781.425.6040  
 Email: [contact@veracode.com](mailto:contact@veracode.com)  
[www.veracode.com](http://www.veracode.com)

SecurityReview is a registered trademark of Veracode, Inc.