VERACODE

WHITE PAPER

Five Best Practices of Vendor Application Security Management

Table of Contents

Executive Summary 1
Managing Risk in the Software Supply Chain 1
Challenges with Securing Vendor Software 3
Taking a Vendor Application Inventory 4
  Assign Business Criticality (Assurance Level) 5
  Designate Security Policy 5
Best Practice 1: Policy Definition 6
Best Practice 2: Communication of Vendor Requirements 7
Best Practice 3: Vendor Commitment and Education 7
Best Practice 4: Test Execution and Compliance 8
Best Practice 5: Learn and Improve Results 8
How Veracode Can Help 9
References 11

Executive Summary

The average enterprise's software ecosystem has become big, complex and insecure. Every organization needs to understand and better manage the risks inherent in its reliance on vendor-supplied software to run the business. Today's vendor-supplied application portfolios often include a heterogeneous mix of installed and cloud-based, commercial and custom-developed, web and mobile solutions.

All enterprises assume some risk in using applications sourced from vendors and suppliers. However, most enterprises assume unnecessary and unmitigated risk by their acceptance of insecure vendor software. Most IT departments do not have the time, budget or internal resources to run a meaningful vendor testing program. Traditional assessment methods are arduous, expensive and do not scale. Vendors are resistant to share access to their software. The result: most enterprises carry too much risk across a software supply chain that includes an average of 300 applications sourced from independent software vendors (ISVs) and other suppliers. The growth in outsourced development over the last decade has only exacerbated this problem.

Many data breaches originate with third-party software. Governance, Risk and Compliance (GRC) efforts are increasingly concerned about the security posture of all applications in the portfolio, with IT/information security personnel held accountable during privacy and security audits. It is imperative that IT vendor management practices extend to application security, and that all software that helps to run the business is analyzed and attested to meet security policy requirements.

Internal IT vendor management and security teams are often overwhelmed by the scope of this problem and could use some guidance in establishing a program that exposes and helps mitigate these risks. This paper details the five best practices to managing a successful compliance program for vendor application security..

Managing Risk in the Software Supply Chain

GRC best practices focus on decreasing potential business uncertainties and legal liabilities for the enterprise. GRC at its most effective is a collaborative effort with disaster recovery, business continuity, finance, enterprise architecture, and security and risk professionals. Increasingly these efforts are impacting IT vendor management processes as regulatory and industry mandates compel increased security and privacy assurances along the software supply chain. Auditors, regulators, and security and risk professionals all have a stake in reducing the risk in IT vendor relationships as a part of good corporate governance.

Today's typical enterprise software supply chains have become increasingly reliant on vendor-supplied applications to run the business. Too often, these externally developed applications contain common security vulnerabilities which expose the organization to cybersecurity risk. Economic, competitive and time-to-market pressures are driving enterprises to use commercial, open source and outsourced code as part of their application development process. The explosive growth of hosted, cloud and mobile apps in recent years has only exacerbated this problem. This mixed code base of unknown security quality increases liability for the enterprise, resulting in an unacceptable level of unrestrained corporate risk.

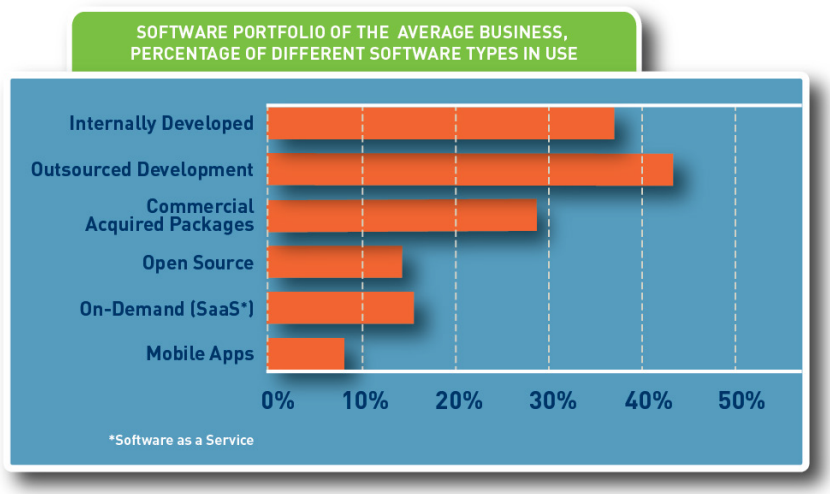

Figure 1: Source: "Outsourcing Software Security", Quocirca Research, April 2012

According to a 2012 study by PWC,[1] less than a fourth of respondents require third-party suppliers or partners to comply with baseline security procedures.. Insecure vendor software is therefore subject to exploitation by hackers and criminals, which puts the entire enterprise at risk of loss of data, revenue, and reputation. The average enterprise has 600 mission-critical applications in its portfolio, with around 65 percent sourced. The result: a typical enterprise carries the risk of more than 300 vendor applications.[2]

To manage this problem, existing GRC efforts must extend to vendor risk management practices. In many industries, regulations such as SOX, PCI DSS, and HIPAA mandate that privacy and security controls extend to a company's software vendors and solution providers. Enterprises must analyze and attest the security posture of all vendor-supplied applications in their portfolio to speed audit compliance and meet policy requirements.

Risk management practices must strengthen software vendor compliance with enterprise IT security policies. This is often best addressed during the software sourcing and procurement process when enterprise customers have more leverage over their suppliers. Suppliers must be convinced that publishing attestation of their software's proven security posture will speed customer acceptance or renewal. Such efforts can also integrate with vendor management practices, where IT manages relationships with network, hardware and software suppliers alike. However, internal IT vendor management and security teams are too often overwhelmed by the scope of this problem.

Challenges with Securing Vendor Software

Enterprises have lacked efficient methods of analyzing the security of their mixed code base. Traditional test methods can be laborious and may cover only a fraction of vendor software in use. Security testing of vendor packages has been limited to manual penetration testing by consultants, internal teams using source code analysis tools, or trusting the ISV, outsourcer or open source project to secure their own code. These approaches fail to deliver an independent verification of application security, scale to cover an enterprise's entire vendor application portfolio, and can add significant time and costs to projects. Examining alternative methods in the table below, it's clear that only an actively managed program that partners with vendors and suppliers to improve application security will garner the best results.

Vendor Application Security Method	Typical Results
Automated test technology with no active program management	Poor vendor outreach, response & remediation rates
Vendor risk management drives with no teeth	Vendors ignore compliance, do not secure software
Testing consultants that can't reach enough vendors	Low number of apps secured as percentage of total portfolio
Expensive programs that do not partner with vendors	Vendor wonders, "What's in it for me?" – protects intellectual property
Do nothing	Risk everything

Another complication is vendor reluctance to expose their source code for security testing in the first place. This circumstance is common, so binary analysis is typically the only simple and cost-effective method to analyze the code statically. Not only does this allow the enterprise to look at the final integrated application without needing source but it offers some inherent advantages for testing for backdoors and malicious code. In all cases regardless of source code availability, assessment should be performed with due consideration of IP rights. As is the case with commercial software, IP rights rest with the vendor. Any assessment the enterprise performs should be done in collaboration with the vendor and include responsible disclosure of any resultant findings. Often it is easiest for an enterprise to avoid any IP violation risks by engaging a trusted independent third-party to perform the assessment and mediate between the vendor and enterprise organizations.

Whether taking on an application security compliance effort alone or with a solution provider, every enterprise must start with an accurate vendor application inventory as a necessary prerequisite.

Taking a Vendor Application Inventory

That which is unknown cannot be secured. In order to secure vendor applications and develop an effective vendor risk management strategy, it is important to understand the underlying diversity and pedigree of the applications in the enterprise's software supply chain. Virtually all enterprise application portfolios are a collection of Software of Unknown Pedigree – an application "SOUP". A typical enterprise software ecosystem consists of a full bowl of internally developed, outsourced, open source, cloud and mobile applications. Furthermore, application development is being carried out by a disparate set of internal and external teams that may have widely varying application security skill-sets, development best practices and security verification standards in place. Protecting your organization from the threat posed by insecure applications means securing this SOUP, including applications acquired from third-parties.

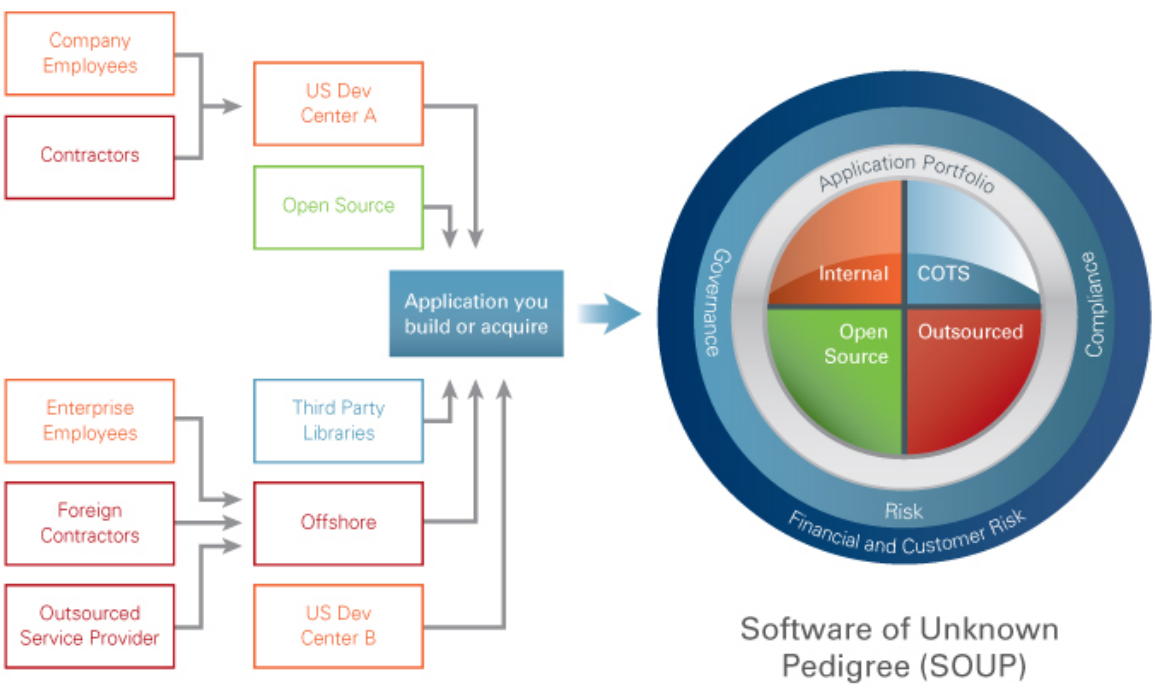

Figure 4: Mixed Application Portfolio of Unknown Security Quality

While it may seem obvious that organizations need an accurate inventory of their vendor application portfolio, in practice it can be a challenging exercise. It is common to see applications in use out of central IT's control as individual groups or business units may have contracted work, purchased commercial applications, or integrated open source or third-party libraries without appropriate cataloging. Business units, procurement and vendor management should be involved when conducting a vendor application inventory to ensure that all software is identified. There are a number of tools on the market that automate the application discovery process by identifying

sets of applications on individual systems and system groups throughout an enterprise network. Results data from such application discovery solutions plus network scanners and lists of purchased SSL certificates can be leveraged as baseline clues to detect additional vendor applications in use. This may not identify all applications, but will provide you with a starting point for your inventory.

Assign Business Criticality (Assurance Level)

It is also important to recognize that not all vendor applications are created equal. Some are simply not business-critical when weighed against common risk factors. Assign an assurance level for each application based on business risk factors such as reputation damage, regulatory impact, financial loss, operational risk, sensitive information disclosure, personal safety, and legal violations. For example, an enterprise engaged in online credit card transactions will need to know which applications in their portfolio are subject to the PCI-DSS regulation and assign those applications a higher assurance level. The following chart from NIST provides guidance on selecting an assurance level based on business risk:

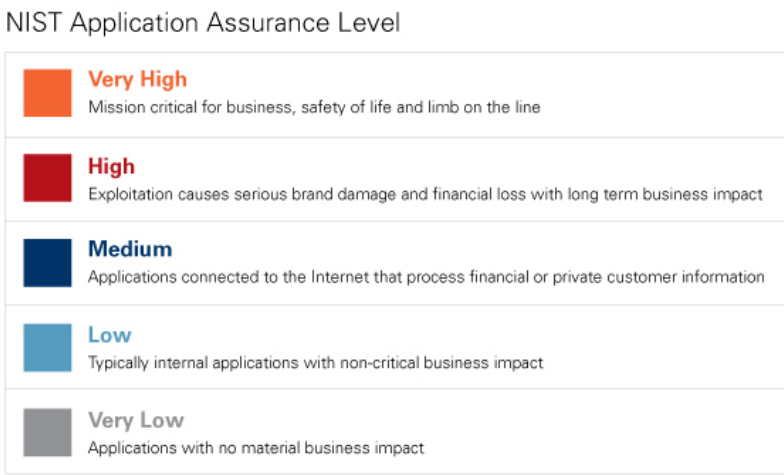

Figure 5: NIST Application Assurance Level Chart

Designate Security Policy

After assigning an assurance level, the next step is to designate a security policy commensurate with the business value of the applications. Since application use cases and potential threats differ from organization to organization, application security policies do as well. They may vary from fulfillment of basic industry standards, such as eliminating OWASP Top 10[3] and SANS Top 25 flaws,[4] to requiring remediation of a detailed list of flaws based on their severity, exploitability and standardized ID.

To demonstrate how security ratings and policies can be applied, we will use Veracode's pre-defined baseline policies as an example. The policies factor in the criticality of the application ("Veracode Level"), various application testing techniques and a scoring system based on the Common Vulnerability Scoring System (CVSS)[5] and the Common Weakness Enumeration (CWE)[6] standards. These three factors produce a "Minimum Veracode Score" for

each application. Thus, enterprises can set an acceptable Veracode Level – "VL3" for example – and outsourcing providers will know what must be achieved for their application to be in compliance.

Setting thresholds and using standards-based scoring removes the subjectivity and "gray-area" for participating vendors and suppliers on what constitutes acceptance while clarifying the process for both the enterprise and testing provider. Below is a chart that demonstrates how organizations can use assurance levels, quality scores and testing methods to achieve an overall rating:

Veracode Level	Flaw Severities Not Allowed in this Level	Required Testing	Minimum Veracode Score
VL5	Very High, High, Medium	Static AND Manual	90
VL4	Very High, High, Medium	Static	80
VL3	Very High, High	Static	70
VL2	Very High	Static OR Dynamic OR Manual	60
VL1	N/A	Static OR Dynamic OR Manual	N/A

In addition to the assurance level and associated security policy, enterprises should also use the application inventory process to capture meaningful meta-data about the application such as origin, development team owner, deployment state, and so on. Documenting these important defining characteristics of your application portfolio will provide a better understanding of the biggest sources of risk, where accountability lies and the most effective security verification and remediation path.

Once all vendor applications have been discovered and ranked by risk level, and after a security policy is in place, only then is a security compliance effort ready to get underway. There are five best practices that every IT organization can follow to ensure that its software security compliance program is set up to succeed with vendors and suppliers.

Best Practice 1: Policy Definition

It is imperative when undertaking any vendor security compliance effort to get the right people in the organization involved early in the process. This should be a cross-functional steering committee reflecting how the enterprise is structured to purchase software. IT security professionals, vendor managers, risk auditors, business unit representatives, sourcing or procurement managers may each deserve a seat at the table. It is also important to confirm who will actually be performing the software testing – internal development, penetration testers, code reviewers, compliance auditors or a third-party solution provider.

Once assembled, the committee should set about defining the enterprise's software security compliance policy, identifying business goals and completing the following:

- Determine what type of security testing is required (i.e. static, dynamic, manual)
- Determine the testing products or services to be used, and how they will safeguard vendors' intellectual property
- Document the analysis timeline and frequency of testing so realistic, achievable expectations can be set with vendors
- Define post-analysis next steps for every possible outcome, with potential impacts on the vendor relationship
- Document vulnerability remediation expectations and acceptance criteria (example: OWASP Top 10 must be passed, and anything that fails must be fixed)
- Document a mitigation process for false positive results, or design mechanisms which override these flaws
- Define an exception and escalation process for uncooperative vendors, which may include non-compliance penalties

Best Practice 2: Communication of Vendor Requirements

Once enterprise policy has been defined, it is time to introduce the software security analysis mandate to all vendors and suppliers. This is best accomplished by the enterprise itself – from the highest level possible such as the CIO or CISO – and should not be outsourced to a third-party solution provider. At the application vendor, it is important to identify the highest value business stakeholder possible – not technical support or development personnel.

This introduction to the effort should position it as strategic – part of the enterprise's unified GRC mandate. It must clearly state the reasons behind the new requirements and the business goals to be achieved. Introduce the vendor to the analysis options available to fulfill security testing compliance. Keep this introduction at a high level and do not overwhelm the vendor with technical details. This is simply a preliminary outreach to promote the program and encourage the vendor's cooperation.

Whenever possible, set up an in-person meeting or live conversation to broker the introduction to the testing team. This will engender trust with the people who will actually be working with the vendor on their compliance efforts. They should leave with a clear understanding of the ancillary benefits of their demonstrated commitment to producing more secure software. These could include a promise to speed future renewal contracts or grant a more formal recognition of "preferred vendor status". Give vendors some time and distance to decide on their course of action – their participation should be positioned as voluntary, but strongly advised.

Best Practice 3: Vendor Commitment and Education

Once a vendor has committed to comply with the application security mandate, a deeper education on the technical aspects of their effort can be undertaken. Provide written guidance that instructs them on all aspects of the analysis process, testing methodologies, expectations and timelines. Allow for a public vetting of the process as outlined and carefully address all questions and concerns in an open, responsive manner. The goal is to obtain a firm agreement from the vendor that they will follow established compliance procedures. Confirm their ability to meet all

requirements in a timely manner as well as their commitment to remediate software vulnerabilities within reasonable deadlines.

Intellectual property protection is one of the most common objections from ISVs when confronting third-party testing regimens. Most are reluctant to allow direct access to their source code by outside parties. It is best to acknowledge this early in the education process and detail how the program plans to safeguard their code.

Best Practice 4: Test Execution and Compliance

Actually administering the enterprise's software security compliance effort often proves the most challenging undertaking. Vendor software must be analyzed, test reports issued and interpreted, vulnerabilities prioritized for remediation, fixes made by vendor development teams, and the software retested to confirm compliance with policy. The enterprise's testing team must provide consistent project management and status reporting to the steering committee to drive the program and minimize delays. To vendors, the testing team drives participation and productivity with accurate results, cooperative methods, and timely response.

Vulnerabilities that pose the highest risk should be given remediation priority. It is important to note that not everything needs to be fixed—just as all applications are not created equal, neither are all vulnerabilities. When reviewing test findings, it is important to consider aspects such as placement and exposure (e.g. external web sites), regulatory impact (e.g. any OWASP Top 10 vulnerability needs to be remediated for PCI compliance), and exploitability (e.g. compensating controls may render the vulnerability less exploitable). The defined security compliance policy will guide and dictate these fixes. This process may offer an opportunity to discuss the vendor's upcoming product releases where the vulnerabilities may have already been addressed or can be addressed. It may also require a discussion around maintenance or renewal contracts where security standards may now be introduced into the contract if they were not previously.

Depending on the severity of the vulnerabilities and the time-to-fix communicated by the vendor or supplier, the enterprise can also make decisions around any intervening compensating controls. These may need to be applied to prevent risk of exploits while the underlying code weakness is remediated and the vendor software brought into compliance.

Best Practice 5: Learn and Improve Results

By maintaining test result derived from these efforts in a centralized repository, benchmarking and trending information can be generated across the entire vendor application portfolio. The enterprise now has the opportunity to get consistent performance metrics across their many vendors and suppliers (e.g. a consolidated view of regulatory compliance). It can identify vendors that are contributing most significantly to its application risk. They can prioritize upgrades to new product releases and optimize contract negotiations by being better informed.

Over time, a vendor application security effort will discover its own efficiencies. For example, some enterprises may be satisfied with summary test reports and allow vendors to limit disclosure of test result details. Some vendors may require a deeper level of advice and remediation guidance from the enterprise's test team during the compliance process. It is critical to build feedback mechanisms into the program so that the steering committee can make any necessary adjustments to maximize the program's success. An honest and open approach to figuring out what is working and what's not working in the program will ensure the highest level of vendor participation and compliance possible.

Developer education is another initiative worthy of consideration. Without clear knowledge of what constitutes good coding practices, many developers will repeat mistakes without knowing it. Enterprises can benefit from online computer-based training services to provide proactive education to the developer and security communities within and beyond their organization. This will not only improve code developed internally, but also allow developers to exercise better judgment when assessing the risks posed by vulnerabilities discovered in vendor code. Enterprises should also investigate the application security education practices in use in their vendor community.

The primary benefit of better visibility into the security state of vendor software is to strengthen the protection of critical enterprise network and data assets. Better cooperation with vendors and suppliers on improved application security can improve IT governance and vendor management practices for the organization beyond software.

How Veracode Can Help

Veracode's Vendor Application Security Testing (VAST) Program provides the first comprehensive application security compliance program to large enterprise customers as well as their software vendors and suppliers. VAST is a completely outsourced solution that combines people, process, and technology.

A VAST Program helps enterprises to better understand and reduce the security risks associated with use of vendor-supplied software, while inviting ISVs and solution providers to participate in the program's success. VAST analyzes and attests to the security posture of vendor-supplied software, while providing detailed, prioritized remediation guidance to the supplier. The program leverages Veracode's cloud-based testing platform which can handle most applications in the enterprise's complete software supply chain regardless of core technology, origin or deployment method.

Veracode's own experience with vendor applications is revealing, and reinforces the need for more disciplined remediation. Our latest State of Software Security report reveals that greater than 83 percent of all applications "flunk" security tests in all cases.

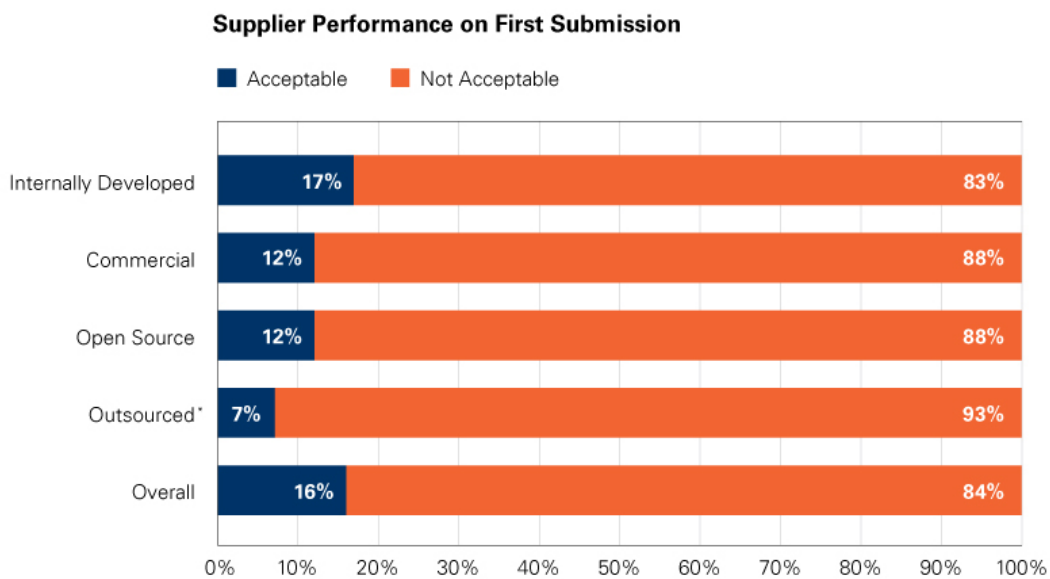

Figure 7: Veracode State of Software Security Report Vol. 4
**Low Sample Size*

What makes VAST unique, however, is that Veracode pursues a systematic course of action that partners with – not punishes – vendors to work together to improve their software security posture. Veracode acts as an independent party providing trust and mutual assurance to the enterprise customer as well as its software suppliers. For vendors participating in the program, Veracode protects their intellectual property rights while verifying their security posture. Detailed, prioritized remediation guidance helps them fix critical security flaws and then confirms their compliance.

Each VAST Program includes:

- A methodical program to achieve application security compliance with as many vendor-supplied applications as necessary.
- Experienced Veracode professional services personnel to guide the enterprise customer, as well as manage and police the program.
- Rigorous security analysis of vendor software, based on industry best practices, but following customer-defined test criteria.
- Visibility into vendor participation tracked and measured against goals, complete with escalation and resolution procedures for improved compliance.
- Final independent attestation that the vendor application meets or exceeds software security policy.

Every VAST Program benefits many enterprise stakeholders. IT security teams can focus and improve their vendor management or risk mitigation efforts. Purchasing and vendor managers can attest the security of externally sourced applications before procurement or acceptance. Compliance officers and IT auditors enjoy speedier examinations, especially in regulated industries such as Financial Services, Retail, and Healthcare.

Veracode has completed thousands of security analyses on vendor applications for enterprises. The VAST Program has been packaged to exploit this collective knowledge for the benefit of the customers we serve.

References

[1] "Third Party Risk Management", PwC, April 2012

[2] "Outsourcing the Problem of Software Security", Quocirca, February 2012

[3] The Open Web Application Security Project (OWASP) is an open-source application security project. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list. The OWASP Foundation is a charitable organization that supports and manages OWASP projects and infrastructure. OWASP Top Ten list: www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[4] The SANS Institute was established in 1989 as a cooperative security research and education organization. It also develops and maintains the largest collection of research documents about various aspects of information security: www.sans.org/top25-software-errors/

[5] CVSS is managed by FIRST, the Forum of Incident Response and Security Teams. The forum brings together a wide variety of security and incident response teams from around the world including product security teams from the government, commercial, and academic sectors. www.first.org/cvss/cvss-guide

[6] CWE is managed by The MITRE Corporation and the co-sponsored by the National Cyber Security Division's Software Assurance program at the U.S. Department of Homeland Security. http://cwe.mitre.org/top25/

WHITE PAPER

VERACODE
Securing the Software That Runs the World

www.veracode.com

Published September 2012

ABOUT VERACODE

Veracode is the only independent provider of cloud-based application intelligence and security verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. By combining patented static, dynamic and manual testing, extensive eLearning capabilities, and advanced application analytics, Veracode enables scalable, policy-driven application risk management programs that help identify and eradicate numerous vulnerabilities by leveraging best-in-class technologies from vulnerability scanning to penetration testing and static code analysis. Veracode delivers unbiased proof of application security to stakeholders across the software supply chain while supporting independent audit and compliance requirements for all applications no matter how they are deployed, via the web, mobile or in the cloud. Veracode works with global organizations across multiple vertical industries including Barclays PLC, California Public Employees' Retirement System (CalPERS), Computershare and the Federal Aviation Administration (FAA). For more information, visit www.veracode.com, follow on Twitter: @Veracode or read the Veracode Blog.