



# vBSIMM Vendor Analysis

## Are your vendors as committed to security as you are?

If your organization relies heavily on third-party software, you're still responsible for making sure it meets compliance requirements and protects customer data. Our vendor analysis puts third-party applications under the same scrutiny as the applications you develop in-house, so you know the code you receive is secure. When your full supply chain is aligned along the same security protocols and practices, you'll decrease risk. Even better, you'll also reduce the time and resources it takes to launch secure software.

### What is vBSIMM?

Vendor Building Security In Maturity Model (vBSIMM) is a metrics-oriented audit that empowers you to measure the software security capabilities within an organization's software development process.

### Why do I need a vBSIMM?

The vBSIMM enables you to retroactively identify and manage the risk of third-party software. Security bugs often creep into software when developers inject "technical debt" into new builds by repurposing code originally developed for other applications or by a third party. The same is likely if they incorporate open source code or components from code libraries into their work. As a result of our vendor analysis, you'll be able to see which vendors you can trust and which need to improve their security posture to continue to be your partner.

### How does a vBSIMM work?

#### 1 Risk ranking

Our team starts by risk ranking the third-party applications, including custom development, commercial off-the-shelf (COTS), and open source. We review vendor documentation and interview your vendors to understand their understanding of software security.

#### 2 Security scoring

We'll assign each of your vendors a security score by looking at five of the 12 practices and 15 of the 112 activities from the Building Security in Maturity Model (BSIMM):

- Architecture analysis (3 activities)
- Code review (3 activities)

Assess the risks inherent to using third-party software.

- Security testing (3 activities)
- Penetration testing (3 activities)
- Configuration management & vulnerability management (3 activities)

### 3 Software testing

Based on the risk of the application itself and findings from the vendor assessment, we then put their software to the test. We may use one or more of the following approaches: static analysis (SAST), penetration testing, or security control design analysis (SCDA).

Only 20% of organizations evaluate the security of third parties with which they share data or network access.

~FS-ISAC

#### Sample vBSIMM questions

Do your vendors have a software security group or at least a designated person in charge of security?

Will they share a documented Secure Software Security Development Lifecycle (SSDL)?

Can they share artifacts that back up the activities described in the SSDL that demonstrate use (for example, results from an architecture risk analysis or a code review)?

How often do they perform security testing?

Who does their security testing? Is it internal or independent?

Will they submit applications to third-party review?

What is their documented process for fixing security defects?

What kind of timeline is involved in remediation and what kind of enforcement is in place?

#### About us

Cigital is now a part of Synopsys, which offers the most comprehensive portfolio of software security solutions in the market. We go beyond traditional testing services to help our clients identify, remediate, and prevent vulnerabilities in the applications that power their business. Our holistic approach to application security offers a balance of managed and professional services and products tailored to fit your specific needs. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure applications. For more information go to [www.synopsys.com/software](http://www.synopsys.com/software).

##### Synopsys Inc.

185 Berry Street, Suite 6500  
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193

International Sales: +1 (415) 321-5237

Email: [software-integrity-sales@synopsys.com](mailto:software-integrity-sales@synopsys.com)