


# BSIMM11 Digest: The CISO's Guide to Modern AppSec






## Introduction

As the rate of software development accelerates, organizations are forced to adopt new practices and undergo cultural shifts. DevOps, with its focus on rapid service delivery, was born of these needs. When done right, the DevOps approach helps build reliable software quickly with fewer roadblocks than agile or waterfall methodologies.

But with change comes challenges. Many organizations have struggled to adapt and improve their application security (AppSec) to keep pace with development cycles. To succeed, AppSec must be integrated into every stage of the development pipeline—in other words, DevSecOps. This requires the right mix of tools, people and processes. Achieving the right balance in each area is a key challenge. Too few tools, for example, leave gaps in their security posture. Too many tools add undue complexity and integration issues that quickly lead to “tool fatigue.”

How can security leaders know how much is too much when it comes to their AppSec activities? How little is too little? What investment makes sense for their particular organization? What investment is overspending or duplicating efforts?

These are the types of questions that Synopsys’ Building Security In Maturity Model (BSIMM) and its annual report were created to answer.




## What is BSIMM?

The annual BSIMM report, now in its 11th iteration, offers CISOs and other security executives a model and framework to test, measure and benchmark their current AppSec activities. Based on the security programs of their peers, BSIMM data offers executives a unique perspective on the state of AppSec and provides insight into the key activities, practices, and tools they should consider implementing in their own organization.

This year’s BSIMM11 report includes data from hundreds of interviews with individuals directly involved in software application security initiatives. It is based on the practices of 130 different organizations across a variety of industries, including financial services, Internet of Things, Cloud, healthcare, insurance, and more. Many of these organizations are household brands such as Adobe, Capital One, General Electric, JPMorgan Chase, The Home Depot, Verizon, and Wells Fargo.

Regardless of how well-known the organization, or mature its AppSec posture, the BSIMM acts as a measuring stick for executives to gauge their own programs against industry trends and other factors. When used to its full capacity, BSIMM functions as a roadmap for creating or improving a successful AppSec program that is tailored to the specific needs of each organization. Executives can identify their own goals and objectives, then layer in BSIMM data to determine where additional effort and investment are needed.



**BSIMM functions as a roadmap for creating or improving a successful AppSec program**

## Key AppSec trends in BSIMM11

Each year, the BSIMM reveals key market trends and what they mean for AppSec leaders. These trends indicate overarching, or more holistic, shifts in how industries approach their application security programs. Executives can review these trends to identify any gaps in their own AppSec programs and determine what additions would be beneficial.

### Development-led vs. Security-led

One of the key findings of BSIMM11 is the extent to which some organizations are shifting toward development-led AppSec programs. Instead of a traditional structure, in which separate security teams drive security, developers themselves are taking on many security responsibilities.

As organizations move toward DevOps, automated tools are removing roadblocks, minimizing errors, and changing the way teams address security. As development speeds increase, teams realize they cannot complete all security activities prior to deployment. This requires a shift in mentality to a “good enough” approach versus a “zero risk” tolerance.

Resilience has become the primary goal within development-led organizations. There is a push for many secure software development lifecycle (SSDL) activities, especially defect discovery and production monitoring and feedback loop activities, to become “business as usual.” Security activities, particularly defect discovery ones such as SAST, SCA and DAST, fit perfectly with existing quality assurance (QA) practices.

### Shift everywhere vs. shift left

The term “shift left” is widely understood to mean promoting security testing early in the development lifecycle. BSIMM11 clarifies this concept to bring it closer to its intended meaning, coining the new phrase “shift everywhere” to underscore the importance of performing security testing as early as possible in every stage of the SSDL. And, as BSIMM11 shows, this approach is increasingly prevalent.

Industry-leading security teams are conducting security activities as quickly and reliably as possible. Continuous, event-based security telemetry throughout a value stream, rather than a single point-in-time analysis, should be adopted as a best practice.

### DevSecOps

The idea of baking security into all phases of a DevOps lifecycle is quickly becoming the norm. But organizations are adopting this approach in their own ways and at their own pace. BSIMM11 notes two key drivers of DevSecOps:

*Software-defined security governance.* Digital transformations across organizations are incorporating security activities throughout their pipelines. This is being enabled, in part, by automation. Organizations that practice a “governance as code” approach have made great strides in streamlining their development pipelines.

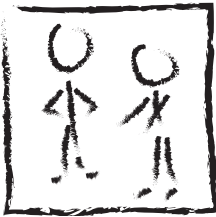


Security as part of a quality practice. Also enabled by automation, practices that have traditionally been performed manually by security team members are being performed by tools and processes throughout the development lifecycle. More and more teams are approaching security as a quality practice, addressing security constantly instead of as the final step before production.

In many organizations, software is built in anticipation of failure, and the associated test cases go directly into regression suites run by QA groups or through automation. Developers and engineers increasingly view security as their responsibility, which means learning esoteric vulnerability and exploitation details, combined with integrating and operating myriad sets of tools to implement security at the speed and scale required for DevSecOps.

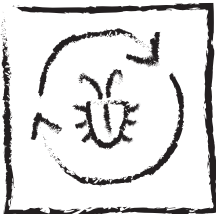
## Emerging AppSec activities in BSIMM11

In addition to reflecting broad sea changes in AppSec, BSIMM also identifies specific activities that are gaining traction and popularity within AppSec programs or initiatives. Given their prevalence across the 130 organizations represented in BSIMM11, it's evident how important these activities are to their respective AppSec programs.



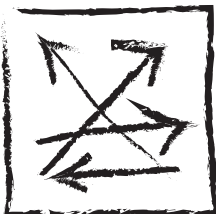
### Governance as code

As stated above, many organizations are successfully replacing manual governance activities with automated solutions. This shift has greatly contributed to increased speed of development across all industries. However, BSIMM11 found that policy decisions must still be made by humans to be effective. The onus is on security teams to understand, modify or add policies in real time to maintain speed and not slow down development.



### Continuous defect discovery

BSIMM11 found that organizations are adopting continuous integration and testing practices into their development pipelines. Such organizations are focusing on creating flexibility by using low-latency and continuous detection loops.



### Continuous activity

The "shift everywhere" approach is moving beyond defect discovery to activities such as configuration governance of containers, APIs, and clouds. Just as software artifacts pass functionally from one lifecycle to the next, so too is security telemetry. Thus, traditional monolithic efforts are being incrementally executed in a stepwise process and automated where possible.



### Security as resilience and quality

BSIMM11 found that organizations are increasingly viewing security through the lenses of resiliency and quality. Improvements to quality assurance and resiliency practices, in the form of people, processes and technology changes, are on the rise. Proactivity is the key takeaway; organizations are adding security activities and resiliency practices to the SSDL to ensure rapid and frictionless vulnerability discovery and mitigation.

# BSIMM11 findings by industry

Each year, BSIMM offers a glimpse into the current success, weakness and maturity of organizations within specific industry verticals. This allows CISOs and other security executives to compare data against their industry peers and pinpoint areas of specific need in their own AppSec programs.

## Important industry comparisons

- **The leaders in maturity:** Internet of Things (IoT), Cloud, and high-technology companies are the three most mature verticals in the BSIMM11 data pool. On average, Cloud organizations are somewhat more mature in their Governance and Intelligence domains compared to high-tech and IoT organizations.
- **Regulated industries:** Financial services, healthcare, and insurance companies all operate in highly regulated environments. BSIMM11 found that large financial institutions reacted to regulatory changes and started their AppSec programs much earlier than insurance or healthcare organizations.
- **Healthcare:** Although healthcare companies increasingly build devices and associated services, their overall maturity trails high-tech organizations that offer similar functionalities.
- **Retail:** Retail companies have lagged behind in their AppSec program development but have made great improvements in the past year.
- **FinTech:** New to the BSIMM model this year, the FinTech vertical compares well to financial services. In fact, FinTech is more mature overall and excels in Training, Code Review and Security Testing practices.

## Using BSIMM to improve AppSec programs

For CISOs new to the BSIMM model, the depth of data and wealth of information can be intimidating. But regardless of size, maturity level or industry, security executives can leverage BSIMM as a roadmap to help develop, improve and mature their AppSec programs. The following activities provide a good foundation or starting point.

### 1. Identify maturity phase

BSIMM defines three maturity phases of an AppSec program. Identifying whether an organization is emerging, maturing or optimizing is a necessary foundation from which to build. Executives should review the common markers below each phase (see chart below) to determine where they currently stand.

Emerging	Maturing	Optimizing
<ul style="list-style-type: none"><li>• An organization starting from scratch or formalizing current adhoc security activities.</li><li>• Initial strategy is defined, foundational activities have been implemented, rough roadmap might be developed.</li><li>• Restraints include budget, lack of resources, lack of talent.</li><li>• 12-24 months needed for evolution.</li></ul>	<ul style="list-style-type: none"><li>• An organization with an existing or emerging AppSec program that is working on scaling, streamlining, and meeting executive expectations.</li><li>• Key activity may include working to apply existing activities to greater % of technology stacks, departments, or software portfolio.</li><li>• Security leadership might add fewer activities, while increasing depth, breadth, and cost-effectiveness of current activities.</li></ul>	<ul style="list-style-type: none"><li>• An organization that is fine-tuning their existing AppSec program.</li><li>• Security management has clear view into operational expectations and associated metrics.</li><li>• Seamless adaptation to technology change drivers.</li><li>• Risk management and business value are clearly demonstrated as differentiators.</li><li>• AppSec leader(s) may be undergoing personal growth from technology executive to business enabler.</li></ul>



## 2. Embrace DevSecOps

Executives must address the role of security within a DevOps environment, which means embracing DevSecOps. Focus should be placed on promoting security self-service for the development team, including automation in the SSDL, and removing points of friction. Speed, agility and automation are key considerations as security must keep up with the pace of DevOps.

## 3. Implement key activities

Activities form the backbone of BSIMM. Each year's report identifies what activities the various organizations in the data pool are performing. The activities are then rated based on frequency. This approach gives CISOs a snapshot into the most widely used activities of their peers.

BSIMM11 found several activities that grew explosively in the past year. Security executives should consider prioritizing these activities since they play a key role in many successful AppSec programs.

New Activities on the Rise					
Activity	BSIMM7 Observations	BSIMM8 Observations	BSIMM9 Observations	BSIMM10 Observations	BSIMM11 Observations
SE3.4 (now SE2.5)	0	4	11	14	31
SE3.5			0	5	22
SE3.6			0	3	12
SE3.7 (now SE2.6)			0	9	36
AM3.3				0	4
CMVM3.5				0	8

**SE2.5** = Use application containers

**SE3.5** = Use orchestration for containers and virtualized environments

**SE3.6** = Enhance application inventory with operations bill of materials

**SE2.6** = Ensure cloud security basics

**AM3.3** = Monitor automated asset creation

**CMVM3.5** = Automate verification of operational infrastructure security

Why are these activities on the rise?

- SE2.5: Organizations are using application containers to make deployment easier and decrease costs
- SE3.5: Organizations are using orchestration for containers and virtualized environments to ensure workloads meet security requirements
- SE3.6: Organizations are leveraging operations bill of materials to enhance their application inventory
- SE2.6: Organizations are ensuring they have cloud security basics in place to keep pace with the overall increase in adoption of cloud-based deployments
- AM3.3: Organizations are monitoring automated asset creation to better understand self-service means of software delivery
- CMVM3.5: Organizations are automating verification of operational infrastructure security to replace some traditional IT efforts, such as application and infrastructure deployment

## 4. Define roles and responsibilities

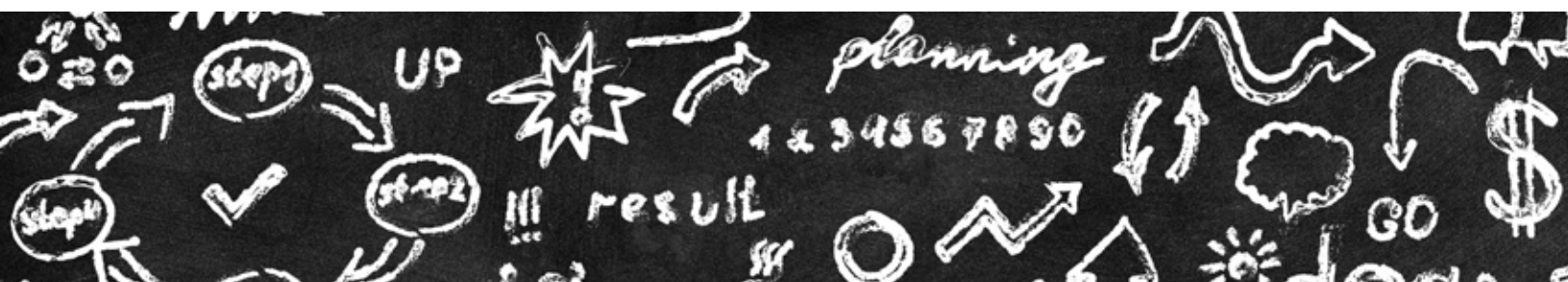
Identifying individuals and their roles in an AppSec program reduces confusion while empowering teams to be proactive and innovative. BSIMM reviews its study subjects each year to determine the key players responsible for application security. As always, success starts at the top; executive leadership is critical. CISOs should review the roles identified by BSIMM to determine if they can create clearer boundaries and expectations in their own organizations.

- **Executive leadership.** The most successful AppSec initiatives are those with executive sponsorship and oversight. Programs gain acceptance and support throughout organizations when they have executive buy-in. And having a single person (typically the CISO) in charge of security decisions allows the program to move forward without bottlenecks.
- **Application security team.** Virtually all 130 organizations observed in BSIMM11 have an established AppSec team in place, though their structure and the names they go by vary greatly. Without this team, organizations would find it impossible to be consistent in their AppSec efforts. Executives should prioritize and closely align with this team to help drive and deliver security goals.
- **Security champions.** Often referred to as “satellites” in BSIMM vernacular, security champions are employees outside the security team who help raise awareness and garner support of AppSec practices among different members of the organization. Executives should identify existing security champions within their organizations and foster relationships with potential champion recruits who can help ensure compliance with AppSec best practices throughout the SSDL.
- **Everyone else.** All employees play an indirect role in security. They can spread awareness, understanding and support for security practices and development. Executives should encourage education, inclusion and awareness across the entire organization to give their AppSec programs the best chance to succeed.

## 5. Getting started

For new CISOs or those in emerging organizations, BSIMM11 provides easy-to-use checklists to help jumpstart an AppSec program.

Security-led checklist for getting started	Development-led checklist for getting started
<ol style="list-style-type: none"> <li>1. <b>Leadership.</b> Put someone in charge of software security and provide the resources they will need to succeed.</li> <li>2. <b>Inventory software.</b> Know what you have, where it is, and when it changes.</li> <li>3. <b>Select in-scope software.</b> Decide what you’re going to focus on first and contribute to its value streams.</li> <li>4. <b>Ensure host and network security basics.</b> Don’t put good software on bad systems or in poorly constructed networks (cloud or otherwise).</li> <li>5. <b>Do defect discovery.</b> Determine the issues in today’s production software and plan for tomorrow.</li> <li>6. <b>Engage development.</b> Identify those responsible for software delivery pipelines, key design, and code, and involve them in the planning, implementation, and roll-out at scale of security activities.</li> <li>7. <b>Select security controls.</b> Start with controls that establish some risk management to prevent recurrence of issues you’re seeing today.</li> <li>8. <b>Repeat.</b> Expand the team, improve the inventory, automate the basics, do more prevention, and then repeat again.</li> </ol>	<ol style="list-style-type: none"> <li>1. <b>Inventory software.</b> Know what you have, where it is, and when it changes.</li> <li>2. <b>Select in-scope software.</b> Decide what you’re going to focus on first and contribute to its value streams.</li> <li>3. <b>Ensure host and network security basics.</b> Don’t put good software on bad systems or in poorly constructed networks (cloud or otherwise).</li> <li>4. <b>Choose application controls.</b> Apply controls that deliver the right security features and also help prevent some</li> </ol>



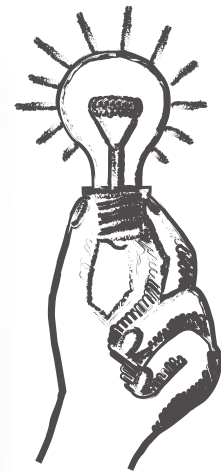
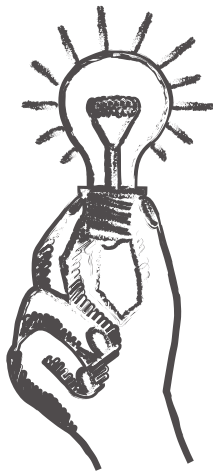
For CISOs overseeing existing programs, BSIMM11 found 12 activities that were most prevalent in highly successful AppSec initiatives. Executives should prioritize these essential activities when reviewing their own programs.

Most Common Activities per Practice	
DOMAIN	DESCRIPTION
Governance	Implement lifecycle governance.
Governance	Identify PII obligations.
Governance	Conduct awareness training.
Intelligence	Create a data classification scheme and inventory.
Intelligence	Integrate and deliver security features.
Intelligence	Translate compliance constraints to requirements.
SSDL touchpoints	Perform security feature review.
SSDL touchpoints	Use automated tools along with manual review.
SSDL touchpoints	Ensure QA performs edge/boundary value condition testing.
Deployment	Use external penetration testers to find problems.
Deployment	Ensure host and network security basics are in place.
Deployment	Create or interface with incident response.

## Next steps

The CISO's mandate is to protect their organization from seen and unseen threats. This requires constant diligence to improve security best practices. BSIMM can be a helpful guide for starting, improving or fine-tuning such practices as they pertain to application security.

While addressing the five activities above, the CISO or security executive should consider diving into the full BSIMM11 report, which contains much greater insight into the activities, practice areas, and domains of the most successful AppSec programs operating today.



[Download the BSIMM11 report now](#)



# The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

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

**Contact us:**

U.S. Sales: 800.873.8193

International Sales: +1 415.321.5237

Email: [sig-info@synopsys.com](mailto:sig-info@synopsys.com)