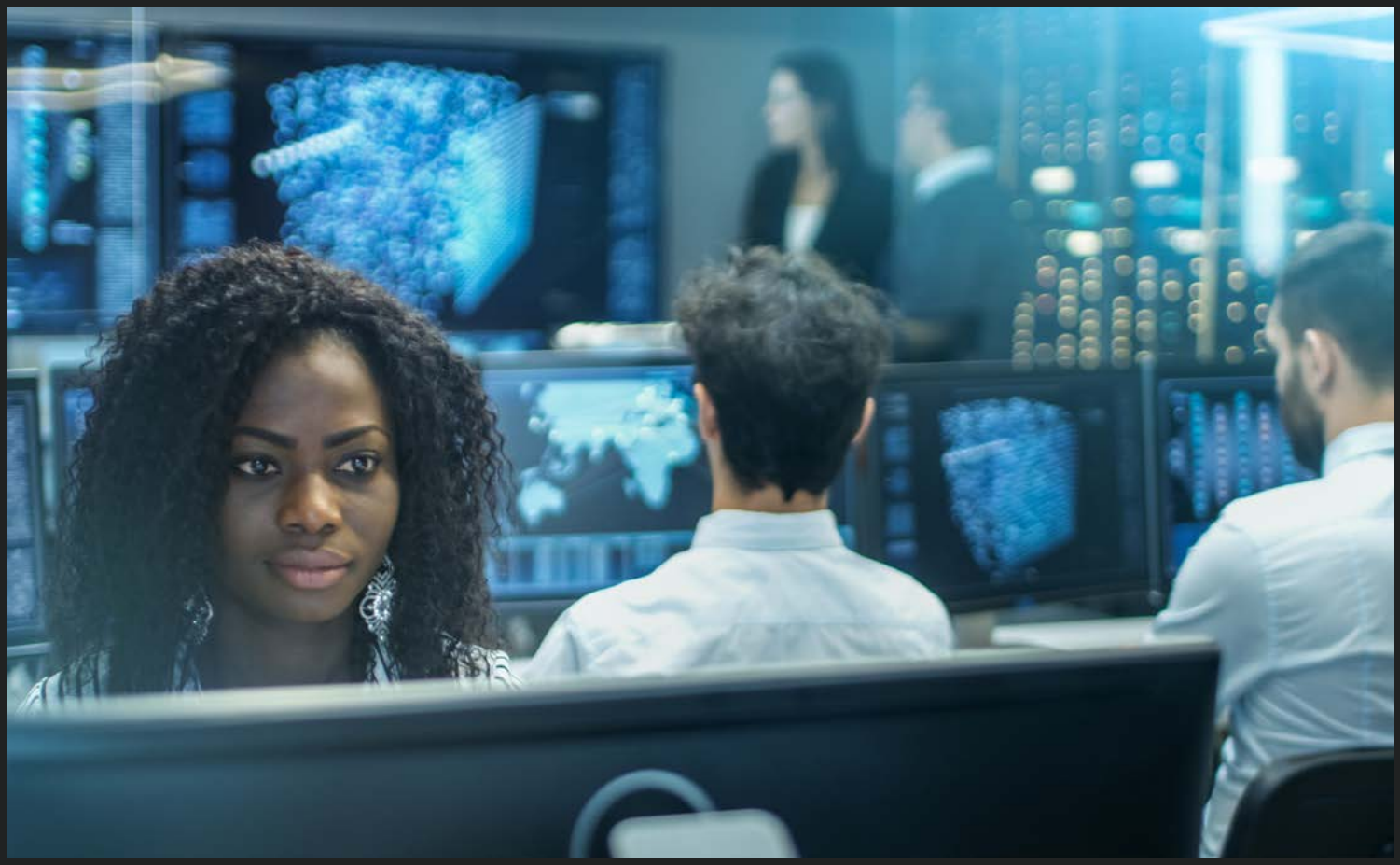
VERACODE



POLICY MATTERS

How to Build a Robust Application Security Governance Framework

An effective application security policy framework can take performance and protection to a higher level

Building a Foundation for Application Security

Over the past decade, application security has emerged as a critical component of business and IT.

A threat landscape that is rapidly changing and increasingly focused on the application layer has ratcheted up risks for organizations. At the same time, business and IT frameworks have become more complex, buying decisions more often occur outside the realm of IT, the pace and complexity of software development have increased, and government and industry regulations increasingly impact organizations.

It's no small challenge for organizations looking to deliver maximum protection for systems and data — and develop quality code that's secure. As a result many organizations are looking to adopt a governance framework that increases protection and decreases risk.

THE OBJECTIVE

1. Simplify and streamline application security

2. Building in maximum protection

Fortunately, these two goals aren't mutually exclusive. When an enterprise addresses policy issues head-on and adopts a robust governance framework, it's possible to ensure that everyone is in-sync, and that the organization is maximizing its investments, interpreting test results effectively and setting expectations for everyone. In the end, this reduces the risk of surprises and performance gaps, helping the organization to lower costs while raising its overall protection level.

Web applications have become the biggest target for attacks.

Why Policies Make a Difference

Organizations are producing apps faster than ever.

And they are augmenting their own development efforts by integrating open-source components and code. In turn, application security governance and policies become critical elements in protecting assets and battling cybercriminals.

Without a strong application security framework in place — essentially the ability to enforce uniform security policies across all applications and portfolios, including third-party libraries — even the best technology and scanning tools will become ineffective thanks to an abundance of test results without any way to prioritize and manage them. This scenario is exacerbated by the current information security labor shortfall.

As organizations move to DevOps and Agile development, the risks can be magnified. Ditto for organizations as they expand into new lines of business and new geographies, which, in turn, may require new compliance requirements, such as PCI, HIPAA, SOX, GLBA, NIST, and MAS. The end result may be bugs, vulnerabilities and a level of exposure that can potentially diminish a brand and adversely impact the bottom line. What's more, a lack of governance introduces an environment where key stakeholders — the board of directors, the C-Suite, line-of-business managers — aren't seeing a clear ROI on an application security program and may lose confidence in the organization's ability to protect itself.

But even if a worst-case scenario doesn't unfold, a lack of governance can result in higher development costs and diminish performance among development teams. Poor or chaotic governance, and a resulting lack of policies, may contribute to a high pressure and high stakes environment where vulnerabilities sneak in due to ad hoc application security methods, and different and sometimes conflicting policies.

In today's business environment, an inability to apply pre-defined policies and enforce custom rules is nothing less than dangerous. It's critical to transform the chaos into order.

Understanding Your Organization's Policy Needs

There's no single path to success in building a governance framework because every organization's policy requirements vary. However, there are a number of common factors that effectively shape an initiative and dictate the overall governance model. Here are several issues to consider:

Absolute Security vs. Program Participation

A common error made by teams constructing an application security policy for the first time is to set the bar too high.

It's important to hold applications to a high standard of security, but it's also essential to recognize that unrealistically high standards will encourage software development teams or third parties to find ways around the policy. This doesn't mean that these organizations don't care about security, but rather, it's a reflection of the fact that attaining security perfection may actually be at serious odds with other business goals, such as time to delivery. A more realistic policy might start with a more attainable goal, such as eradication of certain categories of high severity vulnerabilities, then become more stringent over time.

Remember: *Application security is not a one-time action, but an ongoing exercise. Just like running a marathon, starting too fast will keep you from finishing the race.*

Flaws vs. Vulnerabilities

It's important to recognize that not every coding flaw will leave you vulnerable to a breach, and that different businesses and industries may face entirely different risks.

While it's important to identify flaws that may fall into OWASP Top 10 or the CWE/SANS Top 25, it's even more important to distinguish between flaws that represent a remote risk and those that represent more substantial, real-world risks. In some cases, the likelihood of a vulnerability being exploited may be low, but the potential damage might be great. In other instances, the chance of exploit might be high, but the damage may not be substantial.

Remediation vs. Mitigation

Just as it's important to take a nuanced approach to flaws and vulnerabilities, it's crucial to allocate resources effectively by considering whether its necessary to mitigate a threat or remediate it.

Simply handing teams a tool and asking them to translate the findings into fixes is likely to result in high costs and ineffective protection. The goal isn't to simply perform triage on what the tool reveals — it's to fix what really needs to be fixed, particularly as multiple departments and shared business outcomes enter the picture.

Third-Party Applications

It's no secret that organizations increasingly assemble or purchase applications, rather than building them all from scratch.

Ensuring that applications purchased from external sources are secure — and that they adhere to overall policy requirements — is becoming more critical, and challenging. In fact, for many organizations, regulations require that third-party code conforms to enterprise requirements before it's put into use. As a result, an organization may require input from procurement or legal department before setting policies and establishing development processes and workflows. The end goal is to create reasonable standards that lead to the best possible results.

Internal vs. External Challenges

For many businesses, it's necessary to establish separate internal and external policies based on the use case, type of application or risk profile, or compliance requirements and auditing needs.

In addition, different partners or customers may have different needs from a business or security perspective. Policies must be flexible enough to accommodate these outside players while ensuring that internal systems remain protected.

Open-Source Libraries

The use of open-source code has changed the development and business landscape in profound ways. Within this space it's nothing short of critical to understand how and where code represents a vulnerability and how this plays out in terms of potential risk.

Our research for our recent report, *State of Software Security: Open Source Edition,* found that more than 70 percent of apps contain a security flaw in an open source library on first scan. There are a few key questions security leaders and development teams must ask: Does an open-source library represent a systematic risk? Could a risk appear or grow? If so, what impact might this have on the enterprise?

Role of OWASP Top 10 or SANS 25

These industry standard systems provide a general barometer for software vulnerabilities.

They're extremely valuable tools for tracking threats, but they're most valuable when an organization ties its policies to these systems in a practical way. For example, a business might determine that its goal is to completely eliminate a particular risk that matches common industry criteria or to tie findings to a compliance standard, such as PCI or HIPAA. An organization might also evaluate apps and coding practices based on risks, or auditing considerations.

How to Construct a Framework That Delivers Maximum Protection

Building a strong governance and policy framework requires more than an edict from the CSO or CISO. There's a need for broad input and a real-world understanding of how to match policies with the organization.

In a best-practice scenario, line of business managers and cross-functional teams spanning legal, procurement, DevOps and risk compliance, help weigh criteria, goals, risks and various other factors to develop a coherent and workable approach. This ensures that policies match different classes of applications, as well as the needs and requirements of different units and groups. It also helps build in flexibility, but allows the business to keep things as simple and streamlined as possible.

A basic fact of application security is that any policy should be only as complicated as it needs to be to deliver the necessary results, but no more than that. In fact, the ability to streamline policies goes a long way toward making them more viable and effective for everyone — internal groups, business partners, and others.

In addition, it's important to plug in critical metrics and key performance indicators (KPIs). In the application security arena, these factors typically revolve around policy compliance, flaw prevalence, fix rates and business-and-goal specific metrics. An organization may look at such factors as how many applications meet internal security policies, overall flaw density, how frequently an organization is testing and retesting apps for vulnerabilities, and the scope and types of risk present, and how they map to real-world costs — particularly if a breakdown occurs. An understanding of this framework leads to strong and effective policies.

When this information is available, it's possible to establish a framework that leads to clear ground rules and expectations for development teams, and terms of guidance for other key groups. The result is a clear set of priorities that flow out of these requirements and ultimately match risk and requirements. This, in the end, makes it possible to establish the right set of policies at every level of the organization — and beyond. What's more, these policies establish guidelines and parameters that help an organization identify the right security tools, automation and responsibilities.

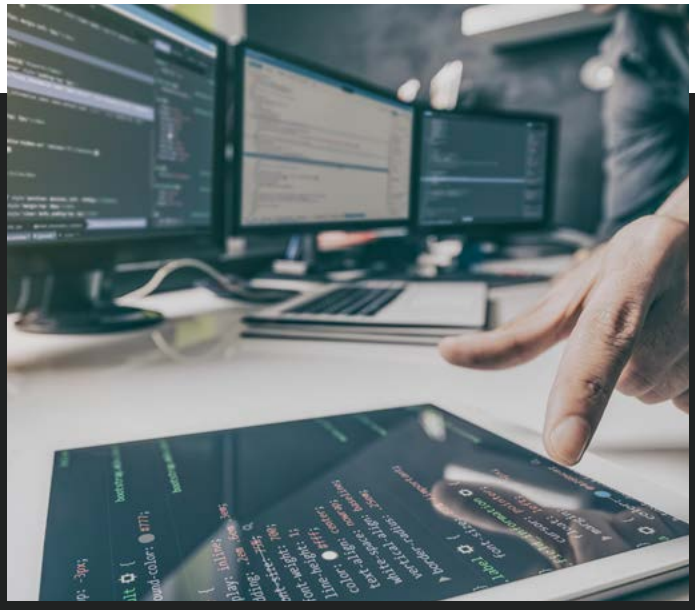
Of course, the security landscape isn't static. As it changes, so must an organization.

As a result it's critical to update policies on a regular basis. Internal changes or new coding requirements, third-party needs or demands, and the overall risk landscape may require an update or full-scale upgrade to policies. Ultimately, the ability of an organization to build an effective policy framework goes a long way toward defining its success with application security.

Application Security Is Written in Code

Success in the application security arena revolves around a strong, yet flexible, governance framework.

If policies are too cumbersome or inflexible, key constituents will undermine or ignore them, thus rendering them essentially useless. However, when organizations assemble the pieces of the puzzle effectively, they're able to reduce risk, minimize conflicts internally and with partners, and build an environment that allows teams to work quickly while reducing risks. This positions an enterprise for maximum protection and maximum results.



LEARN MORE

Get more details in our guide, *Everything You Need to Know About Creating AppSec Policies.*

Veracode is the leading independent AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities. Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode solution has assessed more than 15 trillion lines of code and helped companies fix more than 51 million security flaws.

Learn more at www.veracode.com, on the Veracode blog, and on Twitter.

VERACODE