White Paper

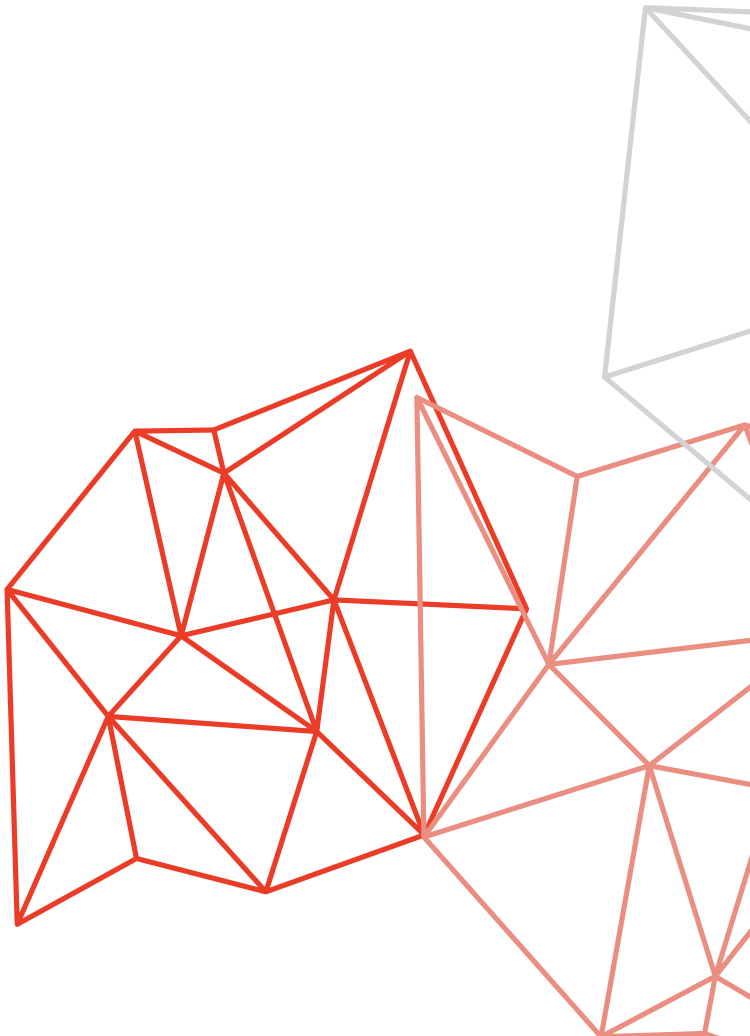
The 5 Fundamental Components of a Secure Application Development Program

Executive summary.

Software security initiatives—a combination of people, policies, and tools—are required by every business that creates or integrates software. These initiatives help to guarantee that programs and the data they handle are safe. Companies are attempting to decide where to begin, how to design a sustainable effort, and what people, procedures, and technology they will require as consumers, regulators, and CEOs and boards of directors begin to demand proof of a formal approach to software security.

A safe development program is the procedure and documentation that software engineers use to create high-quality software products. It also serves as a framework that describes the activities that must be completed throughout each step of software development. When designing and developing apps, organizations may utilize this method to add structure to their efforts.

A good strategy for numerous tasks in software development such as planning, creating (developing), and maintaining software applications is provided by the software development life cycle (SDLC). A approach for improving the overall quality of software applications in a company is also provided.

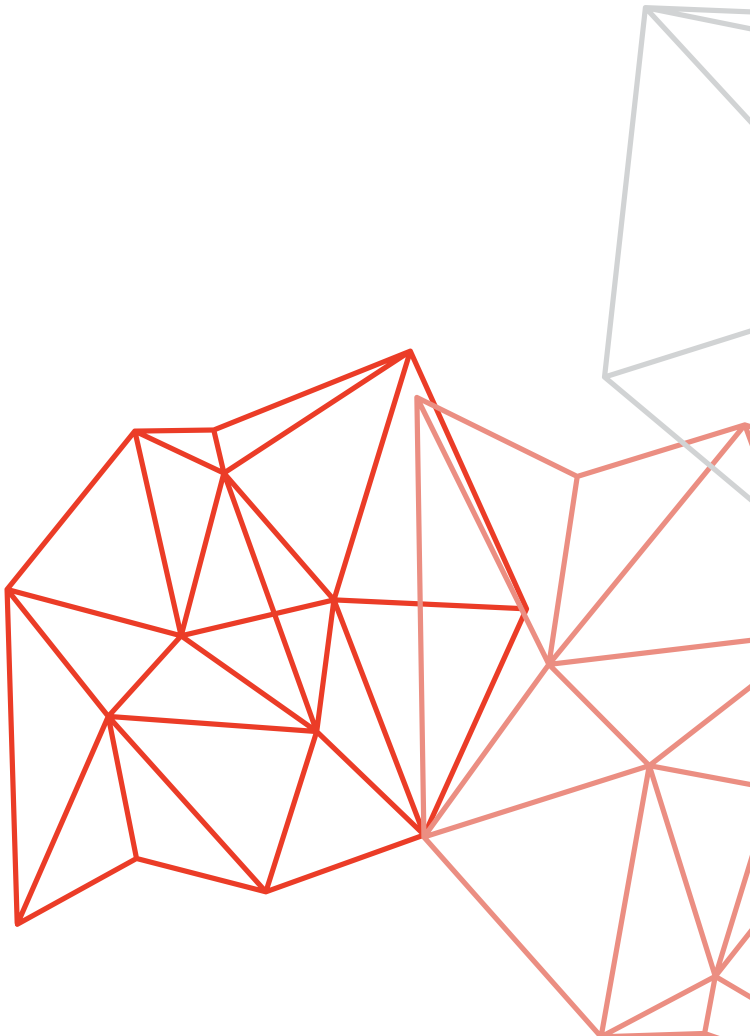


Why have a software security program?

Setting up a software security program has the purpose of improving the security of all deployed software, regardless of whether it was purchased, outsourced, utilized as a service, or produced internally. A disciplined and scalable strategy should be employed to achieve this goal. When stripped down to its most basic components, your initiative is a combination of people who are dedicated to software security (commonly referred to as a Software Security Group), as well as the processes and technologies they use to ensure that your applications are not subjected to unacceptable levels of risk.

A single solution or program does not fit all organizations; instead, each must develop a strategy, establish best practices, and prepare for the appropriate-sized endeavor and degree of effort to fulfill its specific software security requirements and objectives. Software security initiatives do not have to be extremely complicated, time-consuming, or costly to implement. As a matter of fact, there are just five critical criteria that your effort must possess in order to provide substantial and visible changes in your software security posture as rapidly as possible.

Here are The 5 Fundamental Components of a Secure Application Development Program



1 Documentation.

Software security policies and procedures.

It is critical to document your software security policy positions, which specify the business controls that will be used to manage risk across your whole software portfolio of products. Software security policies can include a wide range of topics, including application risk ranking, development project impact ranking, data classification, and data encryption. In addition, these policy statements should establish mandatory objectives and describe what each stakeholder is expected to accomplish.

What should I include in my policies?

It's important for application security policies to explicitly describe what tools, controls, and systems are necessary inside security, even though no single policy can be tailored to meet the needs of every business. As a result, security encompasses both technology and processes, perfectly linking the two together. Businesses should also take into consideration the following factors while developing successful application security strategies.

Prioritization of vulnerabilities

The policy should establish a criterion for determining what comprises high, medium, and low risks. This assists you in determining which vulnerabilities need to be addressed and which should be flagged for further investigation.

Threat history

Analyze which threats and vulnerabilities have had the most severe implications in your technological stack over the course of time. This gives a starting point for consideration.

Roles and responsibilities

Application security roles and responsibilities should be defined in the policy, as well as at what stages of the software development lifecycle (SDLC) they are responsible.

Remediating and mitigating vulnerabilities

This is closely related to vulnerability prioritization, but becomes more precise. Who makes the decision about what needs to be remedied? During what stage of the development process should a vulnerability be addressed? Is there a level of danger that is acceptable?

Remediating and mitigating vulnerabilities

This is closely related to vulnerability prioritization, but becomes more precise. Who makes the decision about what needs to be remedied? During what stage of the development process should a vulnerability be addressed? Is there a level of danger that is acceptable?

Processes

Application security rules should specify the steps that must be followed in order to apply security to application code. Will your company, for example, use SAST and DAST in its operations?

2

Have at least 1 dedicated software security resource.

To guarantee the effectiveness of your software security effort, it is critical that you remove resource limits and offer the infrastructure and skills necessary for personnel to properly support the initiative. If you do not, your initiative will fail. The value of rules, processes, and a charter may be clearly demonstrated by a one-person Software Security Team, which can then grow into a fully-supported team with additional resources.

How do I hire cybersecurity expertise?

What are the advantages and disadvantages of your application security program? Prior to beginning the hiring process, you must determine your needs in order to ensure that any new hires can contribute to filling those gaps.

Recruitment specialists to assist you in strengthening specific areas of your security strategy, or taking a long-term approach and hiring talent who can assist you in mitigating risks in the future and staying one step ahead of the curve, are examples of what this could entail.

It is necessary to have a comprehensive application security strategy in place in order to ensure its success.

One potential vulnerability is one too many, which is why it's critical to hire people who have a diverse range of skills and expertise to ensure that your organization is not vulnerable to a cyberattack.

Don't overhire in one area while leaving several others vulnerable to attack; instead, hire strategically to ensure that all security bases are covered.

3 Train resources.

Software security education and best practices can be distributed throughout your organization through the use of an on-demand training e-library. The ability to scale continuous learning efforts and ensuring that engineers are educated on secure coding methods are two important benefits of this arrangement for your company.

Application security-specific training

It is particularly crucial from a training standpoint to develop competency management competencies. When you educate your employees on security, you can build a competent workforce and instill a culture of software security throughout your firm.

To accomplish this, role-specific training, including computer-based training packages (also known as e-learning), can be undertaken and delivered to you personnel.

Application security training is a preventative measure

Application security education can be used by your organization as a preventative action to keep your software safe and secure. Software security is ruled by black hat security expertise rather than white hat secure software development expertise, according to a recent study. Attack vectors and software-induced security vulnerabilities continue to grow in tandem with the advancement of new technologies, and the industry is battling to keep up with the growing number of threats.

You should already be delivering general cyber awareness training

Despite the increasing threat of cyber assaults, management teams continue to face a significant issue when it comes to Security Awareness Training. Identification of what training has to be delivered, identification of who needs to be trained, and a lack of employee involvement are all frequent difficulties that organizations encounter when attempting to implement Security Awareness Training programs.

Serious considerations should be made to introduce security awareness training, if you are not already delivering it to your personnel.

4

Provide your resources the right tools.

Increase efficiency by assisting developers in fixing security problems before they are deployed to the code base and by avoiding common vulnerabilities from being propagated into the code base. Providing developers with the ability to address problems in real time is less expensive than scanning finished programs programs for faults and entering a fix-and-retest cycle once each fix is performed. Early identification and repair can help to avoid potential delays in product launches and patch cycles, as well as the large expenses associated with each. An excellent solution is to use an integrated development environment (IDE) plug-in that automatically delivers "just in time" security advise as the code is being created. It equips developers with the ability to write secure code the first time, thanks to a program that functions as a desktop security expert, offering automatic help.

Application security-specific training

Performing functional testing of a web application while keeping it under observation is the major role of security testing, and the goal is to identify as many security flaws as possible that might potentially lead to a hacking attempt. All of this is accomplished without the need to view or modify the source code.

The process of security testing aids in the discovery of numerous gaps and faults in a web application during the development stage. Furthermore, it aids in the testing of whether or not a security code has been effectively encoded by an application or not.

There are a variety of free, commercial, and open-source tools available to help you identify and fix vulnerabilities and faults in your web-based software. The nicest thing about open-source technologies, apart from the fact that they are free, is that they may be customized to meet your individual requirements.

5 Implement reporting and remediation.

Provide your senior management with more insight into and governance over the business risk associated with your organization's software assets by acting proactively and consistently. If you want to maintain (or expand) continuous support and resources for your software security program, it is vital that you demonstrate progress from baselines toward targets.

Why cybersecurity governance is important

Traditionally, cybersecurity is regarded through the viewpoint of a technical or operational issue to be managed in the technological sector. Cybersecurity needs to evolve from a back office operational role and move into its own area linked with legislation, privacy and corporate risk. The chief information security officer (CISO) should have a place at the table with the CIO, COO, CFO and the CEO. This move will enable the strongest component of any cybersecurity governance program — the "tone at the top."

This will help the C-suite comprehend cybersecurity as an enterprise-wide risk management problem — along with the legal consequences of cyber hazards — and not merely a technology one. Successively, the C-suite may then establish the proper tone for the firm, which is the cornerstone of every strong governance program. Establishing the correct tone at the top is much more than a compliance exercise.

It guarantees that everyone is operating according to plan, as a team, to deliver business operations and secure the safety of assets within the context of a risk management and security strategy.

Conclusion.

Developing a software security initiative might be frightening, but there are professionals available to expedite the process of building an initiative that can expand and adapt to your increasing software security requirements.

The push to execute a more focused and holistic approach around software security is coming from many directions—from consumers and top executives to regulatory bodies and the organizations in your software supply chain. For all these stakeholders, accepting the dangers of insecure software is no longer an option. Piecemeal goods and services will not reliable enhance your security posture; the cost-effective solution is a software security program that unifies all the separate policies, tools and operations.

More resources available at: https://subrosacyber.com

SubRosa
2000 Auburn Dr
Ste 200 #366
Beachwood OH
44122
888.893.1983
info@subrosacyber.com

Since 2017 SubRosa proudly delivers cyber risk advisory and related services to public, private and government clients.

This brochure is to be used as a reference for general information only, and no content contained herein is designed to provide cyber risk professional advice or services.