

SECURITY PROGRAM IN R&D

WHITEPAPER

July 2025

© 2025 Software AG. All rights reserved.

softwareAG
A SOFTWARE GMBH BRAND

1 Introduction

The value of an organization lies in its assets and security plays an important role in protecting it. It is not enough to have certain security policies alone to secure the IT Infrastructure.

To integrate security within the business processes, an organization needs to have a robust information security program that maps to its business drivers, legal and regulatory requirements, and threat profile.

A security program provides the framework for keeping the company at a desired security level by assessing the risks, deciding how to mitigate them, and planning how one keeps the program and the security practices up to date.

It is a continuous effort that requires the top management's involvement and participation of the personnel from different departments of the organization.

Software AG follows a product development security program that is derived from the practices defined in OpenSAMM Security framework.

This document presents a brief overview of this customized OpenSAMM framework.

It also explains the security practices followed by Software AG to keep the product suite to the required security maturity level.

2 OpenSAMM

OpenSAMM is an open-source framework that helps building an operational and well-organized security program for software development. It helps the organizations formulate and implement a strategy for software security.

The resources provided by OpenSAMM aid in:

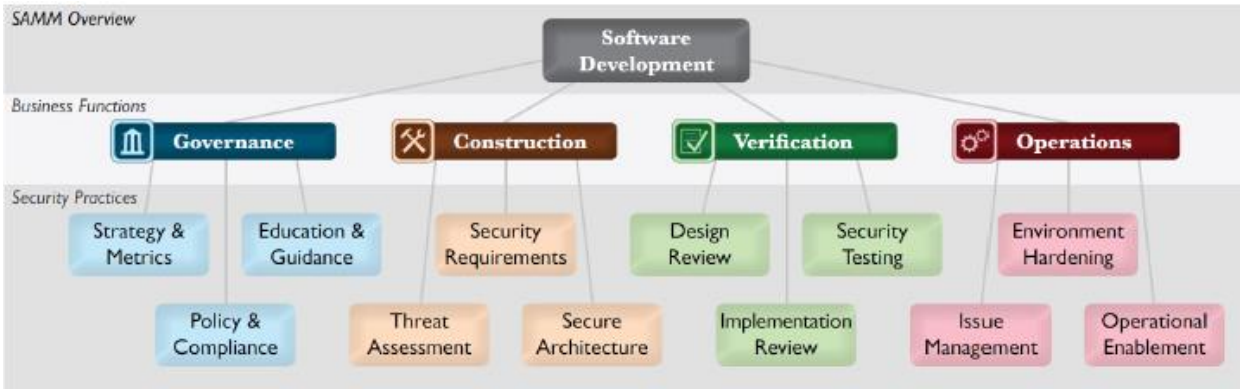
- Evaluating an organization’s existing software security practices.
- Building a balanced software security program in well-defined iterations.
- Demonstrating concrete improvements to a security assurance program.
- Defining and measuring security-related activities within an organization.

At the highest level, SAMM defines four critical business functions. Each business function is a category of activities related to the pre-release activity or the post-release activity in any software development life cycle.

© 2025 Software GmbH. All rights reserved.

OpenSAMM defines three security practices in each SAMM Business Function. Each security practice builds assurance for the related business function.

For each security practice, OpenSAMM defines three maturity levels as objectives. Each level is characterized by a successively more sophisticated objective, defined by specific activities and more stringent success metrics than the previous level.
There are 4 business functions with 12 security practices that are independent silos for improving the map underneath the business functions of software development.



3 Software AG Security Practices

Software AG has adopted the security processes from OpenSAMM framework which takes care of things related to product development security activities in the organization. These processes are tailored to streamline the security related efforts and unify the various products in their level of security.

3.1 Security Metrics Collection & Presentation

OpenSAMM Business Function: **Governance**
Practice: **Strategy & Metrics**

The introduction of the 'Product Security Dashboard' ensures efficient management of security activities within Software AG as it is accessible to both the product as well as security team for structured tracking of issues. The dashboard provides metrics in a readable form that helps the management in:

- Assessing the status and progress of the security activities.
- Allowing the management to evaluate the organization's stand on security.
- Identifying the areas that are improving to make decisions on planning the future investments.
- Measuring the amount of effort taken in developing and fixing the security features or the bugs.

There are several other metrics that are relevant to different people having different roles in planning better security. For example, a graph with information about the list of products

© 2025 Software GmbH. All rights reserved.

categorized by its risk levels can help the Product management decide the level of security required. Based on that, the required security action can be implemented.

The information about the number of open security issues helps the product teams and the security team to plan their upcoming tasks. A scheduled detailed report for each product sent to the product owners and management helps to bring the right visibility and prioritize security issues accordingly.

The report contains released specific data from the dashboard which includes the number of open security defects, static code analysis status, backporting and forward porting defect status, 3rd Party vulnerability defect status and additional statistics on secure design and development metrics.

3.2 Compliance Assessment

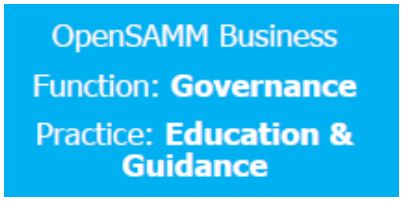


Compliance Driven Security Assessment (CDSA) connects application security and compliance, thus reducing risks to the applications and documenting the compliance of our applications. CDSA provides guidance on specifying, designing, selecting, and implementing information security controls through a set of processes.

The application consists of carefully drafted questionnaires, based on compliance standards, that indicate where a product stands from a compliance perspective. The assessments are of high importance as their purpose is to ensure that all products are developed on top of protection laws, guarantee that the applications deliver the required level of security, and it is in line with the regulatory and industry compliance standards.

Based on the industry requirements, the products are also assessed to ensure that they adhere to data security and data privacy requirements of the data protection acts. The management is responsible for tracking the level of risk associated with an application. The risk increases if an application does not comply with the applicable standards.

3.3 Security Training



As a prerequisite for developing secure software, the teams must be well-versed in information security, including security and privacy issues that may affect the users of the product. The R&D and the Product management staff receive regular security-based training. The training consists of one initial course and multiple refresher courses that help employees to be kept up to date with the current security trends.

The courses are available on Software AG's internal training portal and employees' progress is tracked. The training is mandatory for all R&D employees and is also applicable for new hires. Depending on the requirements of the employee, training can also be conducted in person.

© 2025 Software GmbH. All rights reserved.

Software AG also provides role-specific, specialized targeted training. In addition to this, Software AG conducts externally arranged training sessions by expert trainers on a need basis.

The participants are required to go through an assessment at the end of the course to ensure the effectiveness of the training.

3.4 Security Static Analysis

All products go through an automated source code security static analysis on a regular basis. Running frequent scans integrated with the build ensures faster feedback to developer, thus facilitates efficient maintenance. The source or the binary security scanning is automated using state-of-the-art tools in the industry.

OpenSAMM Business Function: **Verification** Practice: **Security Architecture & Design Review**

This code scanning and analysis is also known as Static Application Security Testing (SAST). The project must be configured once in the central static code scanning system. The tool reads the source code from the central repository and performs the static scan.

The scan displays a list of security vulnerabilities in the code. It also identifies the area of code that can be improved with respect to security. Furthermore, the tool can be configured to perform the scan at regular intervals.

Once the scan is complete, the first pass usually generates a substantial number of false positives. The developers emphasize vulnerabilities, and the security vulnerabilities are mitigated, corrected, or marked for review. As a part of Quality Gate check, for a product to be released, it must not contain outstanding issues.

These issues related to a product are tracked and maintained in the Product Security Dashboard allowing the management to assess the product from a security perspective. Static code results are considered as one of the security release criteria for product release.

3.5 Supply Chain Security Assessment

All the products of Software AG product suite use many 3rd party components. The vulnerabilities in the open-source third-party components are extremely common and could be used to compromise the security of the systems.

OpenSAMM Business Function: **Verification** Practice: **Security Testing**

A continuous scan is performed on these components for detecting vulnerabilities using commercial scanners. If there are issues identified with any of the components used, they are upgraded or replaced before the release.

We regularly scan the product suite and identify the vulnerable components if any. The scan results are reported and followed up with the product development team to upgrade or use an alternate solution.

© 2025 Software GmbH. All rights reserved.

The third-party vulnerability assessment is one of the security release criteria for product release. A procedure is also put into place to scan products containing docker deliverables via commercial tools. Frequent scanning helps minimize the vulnerabilities existing within the product.

3.6 Security Penetration Testing

OpenSAMM Business Function: **Verification** Practice: **Security Testing**

Product Security Penetration testing of an application or product is a method of evaluating the security level of a computer system or network by simulating an attack from attackers (any person who does not have credentials or authorization to access the systems) and malicious insiders (users who have some access rights to the systems). This is performed on the products that expose a web or other network interface.

At Software AG, various activities are involved in penetration testing the components and finding potential vulnerabilities that could result from poor or improper:

- System configuration
- Session management
- Data validation
- Business logic
- Multitenancy

There are two types of penetration testing performed internally at Software AG: Application Penetration Testing (APT) and Network Penetration Testing (NPT).

APT consists of running penetration testing tools against the exposed interface, analyzing the results, and following up with manual penetration tests. This analysis is performed from the perspective of an attacker and can sometimes involve active exploitation of security vulnerabilities.
APT involves use of Dynamic Application Security Testing (DAST) and manual penetration by a skilled internal team. APT is performed on the application runtime and aims at discovering the vulnerabilities in the application and a few of them are listed below:

- Input/output validation such as cross-site scripting (XSS), and SQL injection
- OWASP Top-10 vulnerabilities
- OWASP IoT Top 10
- OWASP API Top 10
- CWE top 25 vulnerabilities
- NIST guidelines

3.6.1 Feature Security Penetration Testing

OpenSAMM Business Function: **Verification** Practice: **Security Testing**

Security Penetration Testing is an important part of application security. This involves evaluating an application by executing it in real time. The focus is to find security vulnerabilities in the new features built into the application. The activities involve testing the features using specific tools

© 2025 Software GmbH. All rights reserved.

and techniques. At software AG, we use industry standards security scanning tools that facilitate automated detection of security vulnerabilities.

3.7 Product Release Standards

Product security verification is performed as part of the Product Release Standards process and is covered with the Security Release Tasks. The objective of the task is to ensure that the products comply with Product Security Policies that are uniform for all the products to reduce the risk of exposure.

OpenSAMM Business
Function: **Governance**
Practice: **Policy & Compliance**

These tasks are created for each of the product teams. The product teams then update and submit the task for analysis. Compliance related checks are performed prior to release via an internal compliance portal. The progress on the release task completion is tracked for each release.

When the product security status task is compliant with the requirements, the product is ready for release from the security point of view. When not compliant, the shortcomings are discussed with the product management and corrective actions are taken to ensure the security of the product.

3.8 Vulnerability Management

Software AG has a well-defined Vulnerability management and Incident Response handling process. Global Support (GS) team is available to provide 24/7 support to customers. Security related incidents or flaws raised by customers are addressed by the GS team if it is in their purview. If an issue needs to be investigated by the R&D team, then the GS team creates specifically tagged bugs in the R&D's bug tracking system.

OpenSAMM Business
Function: **Deployment**
Practice: **Vulnerability Management**

Software AG internally uses CVSS 3.x scoring system for assigning priorities to ensure that the security flaws are handled with adequate priority. The product teams patch the security flaws and release fixes at the earliest. The security fixes are released with limited information along with standard fix packs to avoid disclosing sensitive information to the public. The internal policy and processes ensure backporting and forward porting of security defects to all the affected versions within the internally defined scope.

Further, a security advisory on the flaw and respective mitigations are published on Empower as required. Customers are recommended to subscribe for Security advisory notifications, so that they get informed about the latest updates as soon as they are published.

© 2025 Software GmbH. All rights reserved.

4 Conclusion

Software AG is making great strides in increasing software security assurance by applying the practices described in this white paper. Software AG customers have witnessed a significant improvement in security in the recent decade. The practices were derived and defined from OpenSAMM security practices and are tailored according to the needs of Software AG.

5 Feedback

If you have feedback or questions on this whitepaper, please send an email to devsecurity@softwareag.com

© 2025 Software GmbH. All rights reserved.