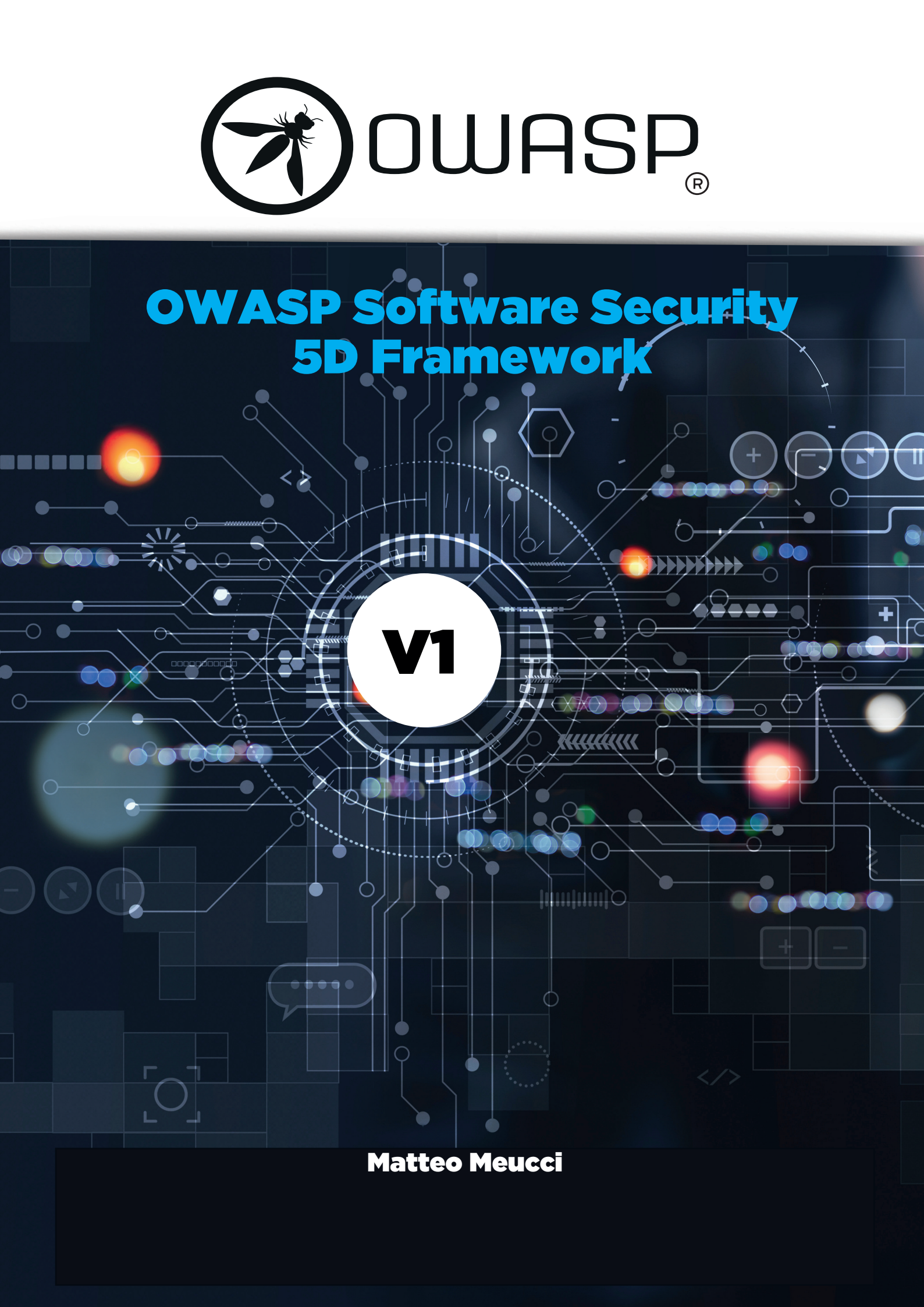

OWASP®
OWASP Software Security
5D Framework
V1
Matteo Meucci

ACKNOWLEDGMENTS

Project Sponsors

We'd like to thank **IMQ Minded Security** (an IMQ Group Company) for supporting the OWASP Software Security 5D project.

Table of Contents

The Open Worldwide Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible", so that people and organizations can make informed decisions about application security risks. Every one is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.

INTRODUCTION

In today's digital era, software security is a crucial aspect of any software development lifecycle (SDLC). In recent years, cyber attacks and data breaches have become increasingly common, and organizations have to be vigilant to secure their applications from such threats. To address this issue, the Open Worldwide Application Security Project (OWASP) has come up with the Software Security 5 Dimension project, a comprehensive framework to evaluate the maturity of an organization's SDLC.

Project Description

The Software Security 5D framework was originally developed by IMQ Minded Security, a leading provider of software security services. The framework is based on years of experience performing software security assessments for various organizations, as well as input from the OWASP community and OWASP SAMM community.

In September 2018, IMQ Minded Security donated the framework to OWASP, making it a part of its comprehensive software security offerings. The framework aims to address the limitations of traditional secure SDLC frameworks, which often lack a level of awareness for all stakeholders involved in the process, a clear description of the application security roles involved, a set of security standards, and security testing tools adopted.

The Software Security 5D framework is a practical framework that focuses on five dimensions to evaluate the maturity of an organization's SDLC. These dimensions are:

SwSec Processes

The SwSec Processes dimension focuses on the processes involved in software development, including requirements gathering, design, coding, testing, and deployment. The framework evaluates whether the organization has a defined set of processes that address software security issues at every stage of the SDLC. It also assesses whether these processes are followed consistently across different teams and projects.

SwSec Testing

The SwSec Testing dimension evaluates the testing procedures used by the organization to identify and mitigate software security risks. The framework assesses whether the organization has a defined set of testing procedures that address software security issues, including vulnerability scanning, penetration testing, and code review. It also evaluates the frequency and thoroughness of these tests and whether they are integrated into the SDLC.

SwSec Team

The SwSec Team dimension evaluates the knowledge and skills of the team members involved in the SDLC. The framework assesses whether the organization has a defined set of roles and responsibilities related to software security, including a security champion, a security officer, and a security team. It also evaluates the training and education provided to team members to ensure they have the necessary knowledge and skills to address software security issues.

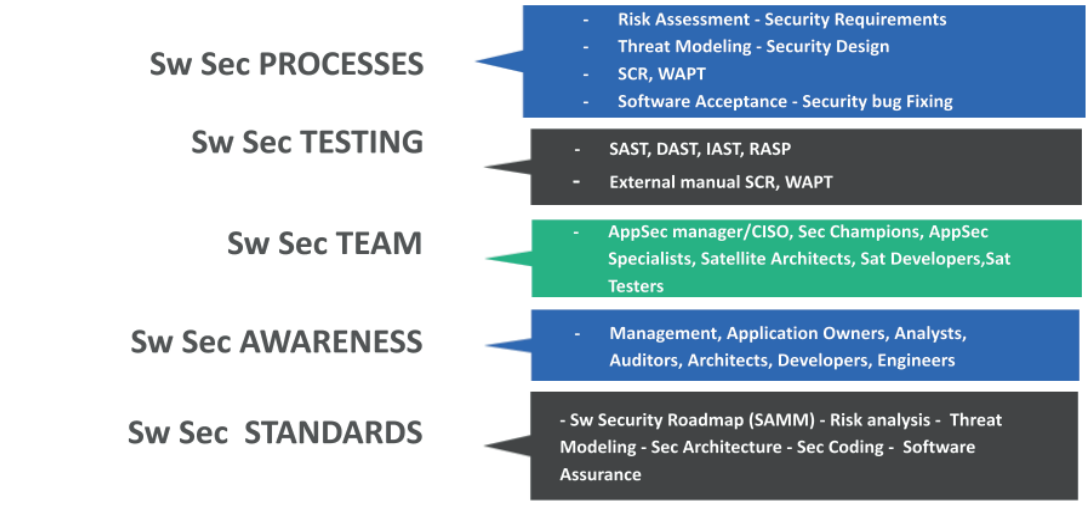
SwSec Awareness

The SwSec Awareness dimension evaluates the level of awareness of software security issues among all stakeholders involved in the SDLC, including developers, testers, project managers, and business stakeholders. The framework assesses whether the organization has a defined set of awareness programs that address software security issues and whether they are regularly communicated to stakeholders.

SwSec Standards

The SwSec Standards dimension evaluates the security standards and guidelines adopted by the organization to address software security issues. The framework assesses whether the organization has a defined set of security standards, including industry standards such as ISO 27001, NIST, and OWASP Top 10. It also evaluates whether the organization has defined guidelines for secure coding practices and secure architecture.

The following picture describe the model at a high level view.



1 | WHY ANOTHER MATURITY MODEL?

1.1 Why another maturity model?

The need for software security frameworks like OWASP SwSec 5D arises from the increasing number of cyber threats that organizations face in today's digital landscape. While there are existing software development life cycle (SDLC) frameworks like the Waterfall model and Agile methodology, these traditional models lack a clear focus on security, which makes them inadequate for addressing security issues in software development. Therefore, OWASP SwSec 5D was developed to provide a more practical framework that focuses on evaluating the maturity of an organization's software development life cycle from a security perspective.

Comparing OWASP SwSec 5D to other software security frameworks, it is worth noting that it is closely related to OWASP SAMM and BSIMM. OWASP SAMM is a maturity model that focuses on software security practices in an organization. It provides a comprehensive guide for software security activities and helps organizations identify their strengths and weaknesses in software security practices. BSIMM, on the other hand, is a benchmarking model that focuses on the maturity of an organization's software security practices by comparing it to other organizations of similar size and industry.

Compared to OWASP SAMM and BSIMM, OWASP SwSec 5D has a more practical approach and focuses on evaluating the maturity of an organization's SDLC based on five dimensions. It addresses the need for a clear focus on security throughout the SDLC, provides a set of security standards, and includes security testing tools adopted by the organization. The five dimensions are SwSec Processes, SwSec Testing, SwSec Team, SwSec Awareness, and SwSec Standards.

In conclusion, OWASP SwSec 5D provides a more practical approach to evaluating the maturity of an organization's software development life cycle from a security perspective. It addresses the need for a clear focus on security throughout the SDLC and provides a set of security standards and testing tools. Although there are other software security frameworks like SDLC, OWASP SAMM, and BSIMM, OWASP SwSec 5D stands out due to its practical approach and its focus on the specific challenges faced by organizations in software development.

The OWASP 5D framework was designed to help companies understand the need to grow in all five dimensions simultaneously, rather than focusing on just one or two. In order to be considered mature, a company must be mature in all five dimensions.

Benefits of the Software Security 5D Framework

The Software Security 5D framework provides several benefits to organizations looking to improve the security of their software development process. These benefits include:

- A comprehensive framework: The framework covers all aspects of software security and provides a comprehensive approach to evaluate the maturity of an organization's SDLC.
- Practical approach: The framework takes a practical approach to evaluate the maturity of an organization's SDLC, focusing on five key dimensions.
- Alignment with industry standards: The framework aligns with industry standards such as ISO 27001, NIST, and OWASP SAMM, providing a recognized set of guidelines.

1.2 | SDLC and SwSec 5D Framework

he Software Development Life Cycle (SDLC) is a methodology used in software engineering to manage the development of software projects. It is a structured approach that divides the software development process into different phases. The SDLC has undergone several transformations over the years, adapting to new technologies and development methodologies.

The Software Development Life Cycle (SDLC) is a process used by software development teams to design, develop, test and deploy high-quality software. The phases of a typical SDLC include:

1. Define:

This is the initial phase where the project scope and requirements are identified, and a project plan is created. The feasibility study is also carried out to determine whether the project is technically and financially feasible.

2. Design:

In this phase, the actual software is designed. This includes designing the software architecture, creating detailed design documents, and creating test plans.

3. Developing:

This is the phase where the actual coding takes place. The software is built, and the development team writes code based on the design documents created in the previous phase.

4. Deployment:

After the software is tested and approved, it is deployed to production environments.

5. Maintenance:

In this phase, the software is maintained and updated. Bug fixes, updates, and improvements are made to the software over time.

Each of these phases has a specific set of tasks and goals, and they are carried out sequentially, with each phase building on the previous one. Properly following a SDLC helps to ensure that software is built on time, on budget, and with a high level of quality.

The OWASP 5D framework is a methodology that can be used in conjunction with any SDLC methodology. It provides a structured approach to software security and addresses the need for security to be integrated into the software development process. The OWASP 5D framework focuses on five dimensions of software security, namely SwSec Processes, SwSec Testing, SwSec Team, SwSec Awareness, and SwSec Standards.

The table in the following page describes the relationship between SDLC phases and all the 5 dimensions of the framework we are describing:

SwSec 5D and SDLC

SDLC phases / SwSec 5D	1. SwSec Processes	2. SwSec Standards	3. SwSec Testing	4. SwSec Team	5. SwSec Awareness
Define	Risk Assessment Secure Requirement	Sw Security Roadmap (SAMM) Risk analysis Secure Software Requirements		Management Security Champions	Management, IT Managers,App Owners
Design	Threat Modeling Secure Software Design	Threat modeling use cases Secure Architecture		Analysts Security Champions	Sec Specialists
Develop	Secure Code Review Web Application Testing Security Bug Fixing	Secure Coding Guidelines Outsourcing Governance (Software Assurance)	SAST DAST IAST SCR	DevOps Security Champions	Devs Sec Specialist
Deploy	Secure Software Testing & Acceptance Security Bug Fixing	Security Validation and Testing	RASP SCR/WAPT	DevOps Security Champions	Ops
Maintain	Secure Software Deployment & Maintenance Security Bug Fixing	Secure Deployment	RASP WAPT	Devops Security Champions	Sec Engineers

**Figure: OWASP SwSec 5D and SDLC*

The table shows how the 5D Framework can be integrated in the 5 phases of the standard SDLC process. For example in the Develop phase of SDLC we can have 3 SwSec Processes in place (Secure Code Review, WAPT, and Bug Fixing), 3 SwSec Standards (Secure Coding Guidelines, Outsourcing Governance), 4 SwSec practices (SAST, DAST, IAST, SCR), 2 roles of the team involved (DevOps and Security Champion), and we need awareness on the DevOps team.

Secure Software Development Lifecycle (SSDLC) is a methodology used by organizations to integrate security into the Software Development Lifecycle (SDLC) process. This approach ensures that security is considered at every stage of the software development process and not just as an afterthought.

The concept of Secure SDLC emerged in response to the growing number of security breaches resulting from vulnerabilities in software. It became clear that traditional SDLC processes did not sufficiently consider security, and as such, a new approach was needed. The goal of Secure SDLC is to identify, prevent, and remove security vulnerabilities early in the software development process, reducing the cost and impact of security incidents.

The implementation of Secure SDLC can vary depending on the organization, but generally, it involves the integration of security activities throughout the SDLC stages. The stages usually include planning, requirements gathering, design, coding, testing, deployment, and maintenance. The Secure SDLC approach typically involves the use of security requirements, threat modeling, secure coding practices, security testing, and security reviews.

OWASP 5D Framework can be integrated into the Secure SDLC approach to ensure that software security is considered in every dimension of the SDLC. The 5D Framework emphasizes the importance of growing in all 5 dimensions simultaneously and avoiding focusing on only one or two areas. The 5 dimensions include SwSec Processes, SwSec Testing, SwSec Team, SwSec Awareness, and SwSec Standards.

2 | THE SWSEC 5D MODEL

The OWASP Software Security 5D framework is designed to help organizations focus on the key areas of software security that are important for managing software security risks throughout the software development life cycle (SDLC). The framework consists of five dimensions, which are SwSec PROCESSES, SwSec TESTING, SwSec TEAM, SwSec AWARENESS, and SwSec STANDARDS.

Each dimension covers specific areas related to software security, such as risk assessment, security requirements, threat modeling, security testing, team roles, security training, and security standards. By focusing on these dimensions, organizations can ensure that software security risks are managed effectively and that software is developed and maintained with security in mind.

The ultimate goal of the framework is to help organizations improve their software security posture and reduce the risk of cyber attacks and data breaches. By adopting the OWASP Software Security 5D framework, organizations can ensure that they have a comprehensive and practical approach to managing software security risks throughout the software development life cycle.

Let's have a look the details of the 5 Dimensions:

2.1 | SwSec PROCESSES

SwSec PROCESSES is one of the five dimensions of the OWASP Software Security 5D framework. It covers the processes that organizations use to manage software security risks throughout the software development life cycle (SDLC). This includes various activities such as risk assessment, security requirements, threat modeling, security design, software acceptance, and security bug fixing. Risk assessment involves identifying potential security risks and determining their likelihood and impact. Security requirements define the security features and controls that should be implemented in the software. Threat modeling is a process of identifying potential security threats and vulnerabilities and designing security controls to mitigate them. Security design involves implementing security controls and measures to protect the software. Software acceptance ensures that the software meets the security requirements and standards. Finally, security bug fixing involves identifying and fixing security bugs and vulnerabilities in the software.

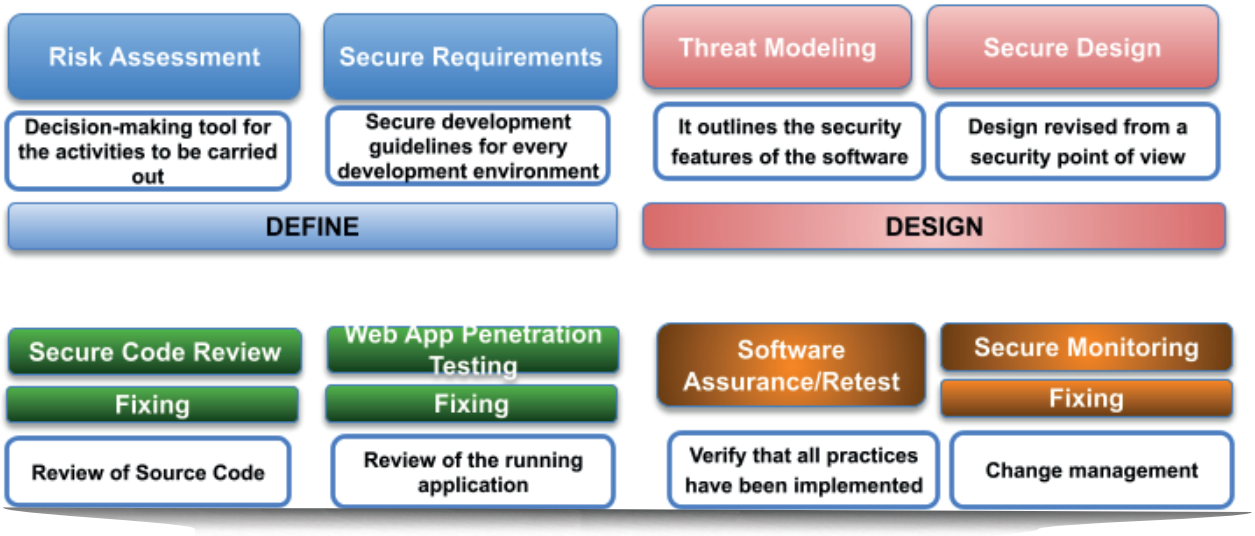


Figure: SwSec 5D Processes

The first dimension focuses on the following assets:

Risk Assessment

Risk assessment involves identifying, evaluating, and prioritizing potential risks to the security of the software system. This can help organizations determine the appropriate security controls and measures to mitigate these risks.

Security Requirements

Security requirements specify the security features, controls, and measures that must be incorporated into the software system to ensure its security.

Threat Modeling

Threat modeling is the process of identifying potential threats to the software system and developing countermeasures to prevent or mitigate them.

Secure Design

Secure design involves developing a secure architecture and design for the software system that incorporates security best practices and principles.

SCR, WAPT

SCR (Secure Code Review) and WAPT (Web Application Penetration Testing) are methods used to identify vulnerabilities in the software code and web applications, respectively.

Software Acceptance

Software acceptance involves testing and verifying that the software system meets the specified security requirements and that it is secure and reliable.

Security bug Fixing

Security bug fixing involves identifying and fixing security vulnerabilities and weaknesses in the software code and system to ensure its security and reliability.

2.2| SWSec Team

SwSec TEAM dimension focuses on the team members involved in software security. This includes AppSec managers or Chief Information Security Officers (CISOs), security champions, AppSec specialists, satellite architects, satellite developers, and satellite auditors. The AppSec manager or CISO is responsible for overseeing the software security program and ensuring that it is integrated into the organization's overall security strategy. Security champions are team members who promote and advocate for software security within their teams. AppSec specialists are security professionals with specialized knowledge and skills in software security. Satellite architects, developers, and auditors are team members who work on specific projects or applications and are responsible for ensuring that the software is designed, developed, and tested with security in mind.

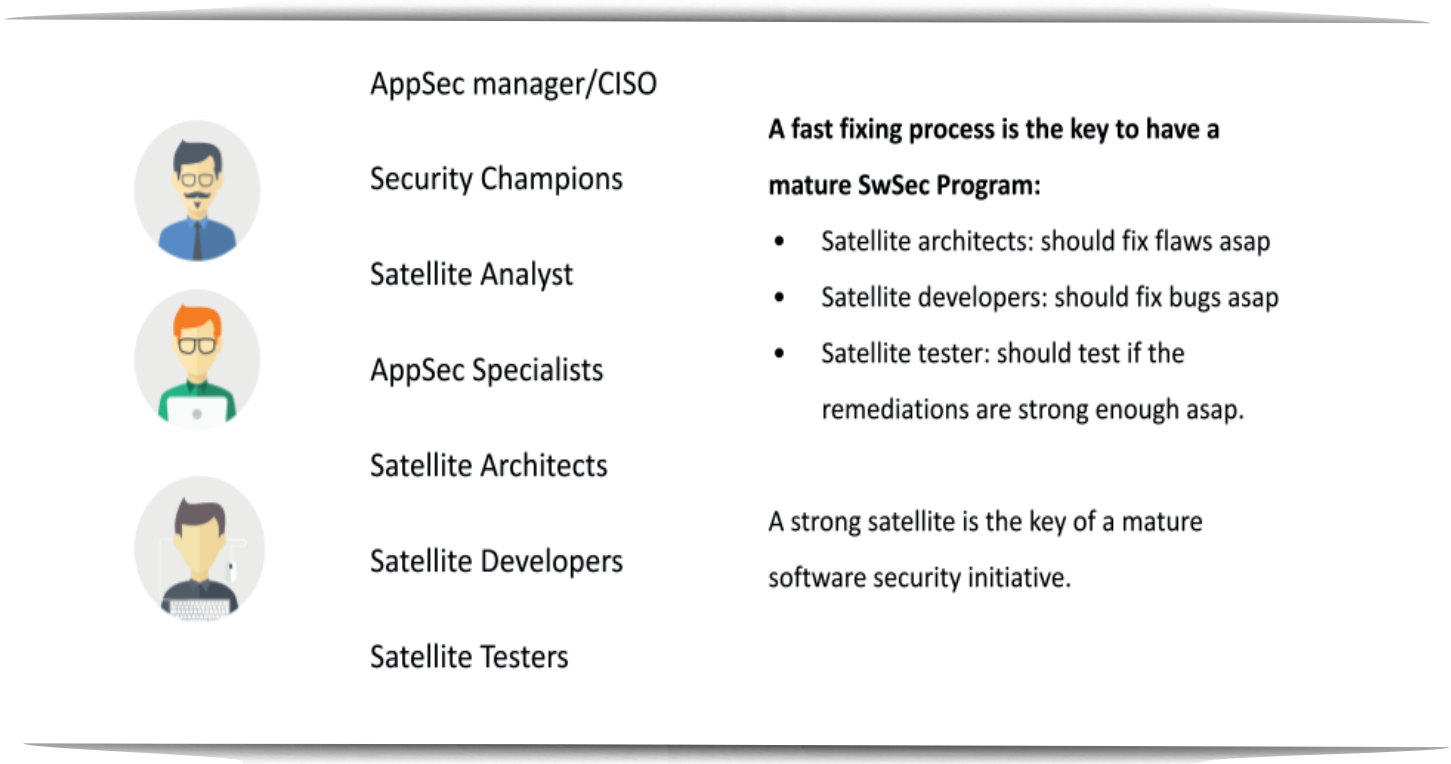


Figure: SwSec 5D Teams

The third dimension of the OWASP Software Security 5D framework focuses on the roles and responsibilities of individuals within an organization responsible for software security. The following roles are essential to building and maintaining a robust software security program:

AppSec manager/CISO

The Application Security (AppSec) Manager or Chief Information Security Officer (CISO) is responsible for overseeing the software security program within an organization. They develop policies, procedures, and guidelines for secure software development, identify and mitigate security risks, and ensure compliance with relevant regulations and standards.

Security Champions

Security champions are individuals within the development or engineering team who are passionate about software security. They act as a bridge between the AppSec team and the development team, advocating for secure coding practices and helping to raise awareness of security issues.

AppSec Specialists

Application security specialists are experts in software security who work closely with the development team to identify and mitigate security risks throughout the software development lifecycle. They provide guidance and support for secure coding practices, perform security assessments, and develop and implement security controls.

Satellite Architects

Satellite architects are responsible for designing and implementing secure architectures for satellite systems or components. They work closely with the AppSec team and the development team to ensure that the satellite system or component is designed and implemented with security in mind.

Satellite Developers

Satellite developers are responsible for developing and testing software for satellite systems or components. They work closely with the AppSec team and the satellite architects to ensure that the software is developed with security in mind.

Satellite Auditors

Satellite auditors are responsible for auditing the satellite system or component to ensure that it meets security requirements and standards. They work closely with the AppSec team and the development team to identify vulnerabilities and weaknesses and develop and implement security controls.

These roles are essential to building and maintaining a strong software security program. Each role plays a critical part in ensuring that the software development process is secure and that software systems are designed, developed, and tested with security in mind. By having dedicated individuals in these roles, organizations can mitigate security risks and ensure that their software systems are secure and resilient to cyber attacks.

2.3| SWSec AWARENESS

SwSec AWARENESS dimension focuses on the awareness and training of team members involved in the software development life cycle. This includes management, application owners, analysts, auditors, architects, developers, and engineers. Organizations can provide security training to team members to improve their understanding of software security risks and how to identify and mitigate them. By raising awareness about software security, organizations can promote a culture of security and ensure that team members understand the importance of software security throughout the SDLC.

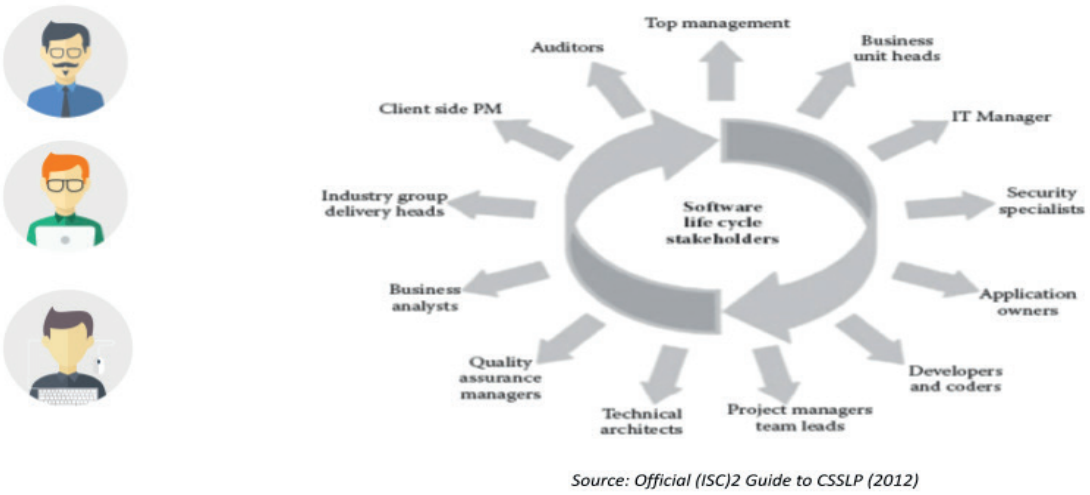


Figure: SwSec 5D Awareness

The fourth dimension of the OWASP Software Security 5D framework focuses on software security awareness, which is crucial to ensure that all stakeholders in the software development process are aware of their responsibilities regarding software security. The following roles need to be aware of software security risks and practices:

Management

Management needs to be aware of the importance of software security and how it impacts their organization. They need to understand the risks associated with software vulnerabilities and the potential impact on their business. Management also needs to ensure that adequate resources are allocated to the software security program.

Application Owners

Application owners need to be aware of the importance of software security for their applications. They need to understand the risks associated with vulnerabilities in their applications and how they can impact their business. Application owners also need to ensure that their applications are developed and maintained in compliance with relevant security policies and standards.

Analysts

Analysts need to be aware of the risks associated with software vulnerabilities and the potential impact on their organization. They need to understand the importance of security testing and the role it plays in mitigating security risks. Analysts also need to ensure that vulnerabilities are identified and addressed in a timely manner.

Auditors

Auditors need to be aware of the risks associated with software vulnerabilities and the potential impact on their organization. They need to understand the importance of security testing and the role it plays in mitigating security risks. Auditors also need to ensure that software systems are audited regularly to identify potential vulnerabilities.

Architects

Architects need to be aware of the importance of security in software design. They need to understand the potential risks associated with design decisions and how they can impact the security of the software system. Architects also need to ensure that security is incorporated into the design of the software system.

Developers

Developers need to be aware of the risks associated with software vulnerabilities and the potential impact on their organization. They need to understand secure coding practices and the importance of security testing. Developers also need to ensure that they write secure code that is resistant to vulnerabilities.

Engineers

Engineers need to be aware of the risks associated with software vulnerabilities and the potential impact on their organization. They need to understand secure engineering practices and the importance of security testing. Engineers also need to ensure that they design and build systems that are secure and resilient to cyber attacks.
Overall, software security awareness is essential for all stakeholders in the software development process. By being aware of their responsibilities regarding software security, stakeholders can help ensure that software systems are designed, developed, and tested with security in mind. This can help mitigate security risks and ensure that software systems are secure and resilient to cyber attacks.

2.4| SWSec TESTING

SwSec TESTING is another dimension of the OWASP Software Security 5D framework that focuses on testing and evaluating the security of software. This includes the adoption of tools such as static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), and runtime application self-protection (RASP). These tools can help organizations to identify security vulnerabilities in their software at different stages of the SDLC. External manual SCR (Security Code Review) and WAPT (Web Application Penetration Testing) are also included in SwSec TESTING to ensure that the software is thoroughly tested and evaluated for potential security risks.

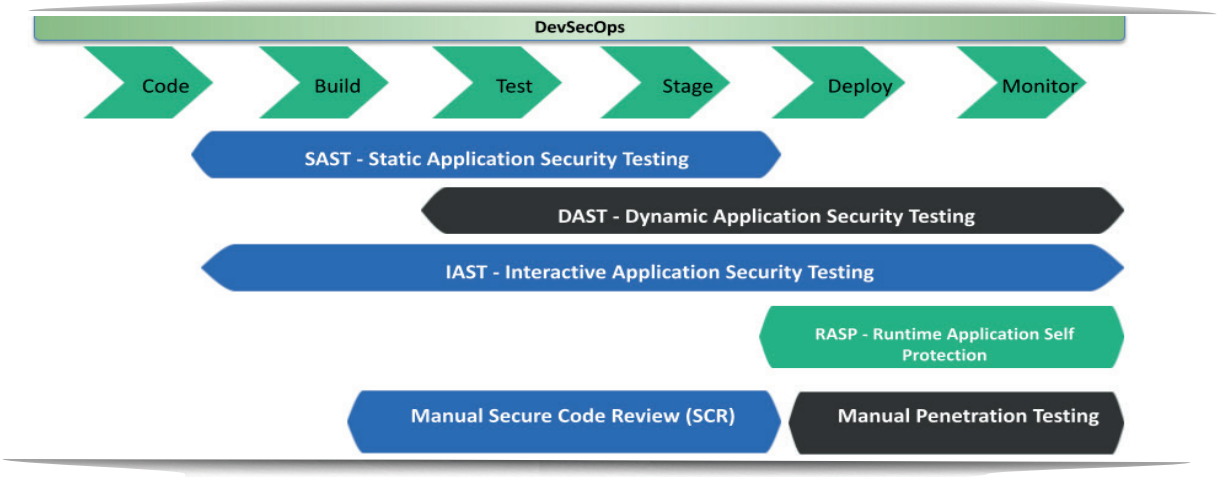


Figure: SwSec 5D Testing

Testing dimension investigates on the following practices:

Adoption of tool like: SAST, DAST, IAST, RASP

There are several types of software security testing, including static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), and runtime application self-protection (RASP).

SAST is a type of software security testing that involves analyzing the source code of an application to identify vulnerabilities and weaknesses. It is typically performed during the development phase

and involves analyzing the code without executing it. SAST tools can identify a wide range of vulnerabilities, including buffer overflows, injection flaws, and cross-site scripting (XSS) vulnerabilities. SAST can help developers identify and fix vulnerabilities early in the development process, reducing the cost and time required to fix them later.

DAST is a type of software security testing that involves testing the running application from the outside to identify vulnerabilities and weaknesses. It is typically performed during the testing phase and involves sending requests to the application and analyzing the responses. DAST tools can identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and broken authentication and session management (BASM) vulnerabilities. DAST can help organizations identify vulnerabilities that may not be found during SAST testing.

IAST is a type of software security testing that combines elements of both SAST and DAST testing. It is performed during the testing phase and involves testing the running application while monitoring the application's behavior at the code level. IAST tools can identify vulnerabilities that may be missed by SAST or DAST testing, such as vulnerabilities related to business logic or custom code.

RASP is a type of software security testing that is performed during runtime. It involves monitoring the application's behavior during runtime to identify and mitigate attacks in real-time. RASP tools can detect and block attacks, such as injection attacks or cross-site scripting (XSS) attacks, before they can cause damage to the application. RASP can help organizations identify and respond to attacks in real-time, reducing the risk of damage to the application and data. Adopting a combination of these software security testing tools can help organizations identify and mitigate vulnerabilities and threats in their software systems throughout the software development life cycle. By incorporating these tools into their software development process, organizations can reduce the risk of cyber attacks and data breaches, improve the security and reliability of their software systems, and build trust with their customers and stakeholders.

External manual SCR, WAPT

External manual security code review (SCR) and web application penetration testing (WAPT) are two important types of security testing that can help organizations identify vulnerabilities and weaknesses in their software systems. Unlike automated testing tools, which can identify a wide range of vulnerabilities, manual testing can identify vulnerabilities that are specific to an organization's software environment.

SCR involves a manual examination of the source code of an application by a security expert to identify security vulnerabilities and weaknesses. The security expert examines the code to identify vulnerabilities such as buffer overflows, injection flaws, and cross-site scripting (XSS) vulnerabilities. SCR can help organizations identify vulnerabilities that may not be detected by automated testing tools, as it involves a deeper understanding of the software system and its components.

WAPT is a manual testing technique that involves simulating attacks on a web application to identify vulnerabilities and weaknesses. It is performed by security experts who attempt to penetrate the web application and access sensitive data or functionality. WAPT can identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and broken authentication and session management (BASM) vulnerabilities. WAPT can help organizations identify vulnerabilities that may not be detected by automated testing tools or manual SCR, as it involves an active attempt to penetrate the web application.

Both manual SCR and WAPT testing require specialized expertise and can be time-consuming and costly. However, they can provide a high level of assurance that the software system is secure and resilient to cyber attacks. Organizations can benefit from manual testing by identifying vulnerabilities and weaknesses that may not be detected by automated testing tools, reducing the risk of data breaches and cyber attacks, and building trust with their customers and stakeholders.

External manual security code review and web application penetration testing should be considered as an important part of a comprehensive software security testing program. By incorporating these manual testing techniques into their software development process, organizations can identify vulnerabilities and weaknesses in their software systems and take proactive steps to mitigate these risks.

2.5| SwSec STANDARDS

SwSec STANDARDS dimension focuses on the standards and guidelines that organizations use to manage software security risks. This includes the OWASP Software Assurance Maturity Model (SAMM), risk analysis, threat modeling, secure architecture, secure coding, and software assurance. The OWASP SAMM provides a framework for organizations to measure and improve their software security maturity. Risk analysis and threat modeling are used to identify potential security risks and vulnerabilities in the software. Secure architecture and secure coding guidelines provide best practices for designing and developing software with security in mind. Software assurance includes various activities such as testing, auditing, and code reviews to ensure that the software meets the security requirements and standards. By following these standards and guidelines, organizations can improve their software security posture and reduce the risk of cyber attacks and data breaches.

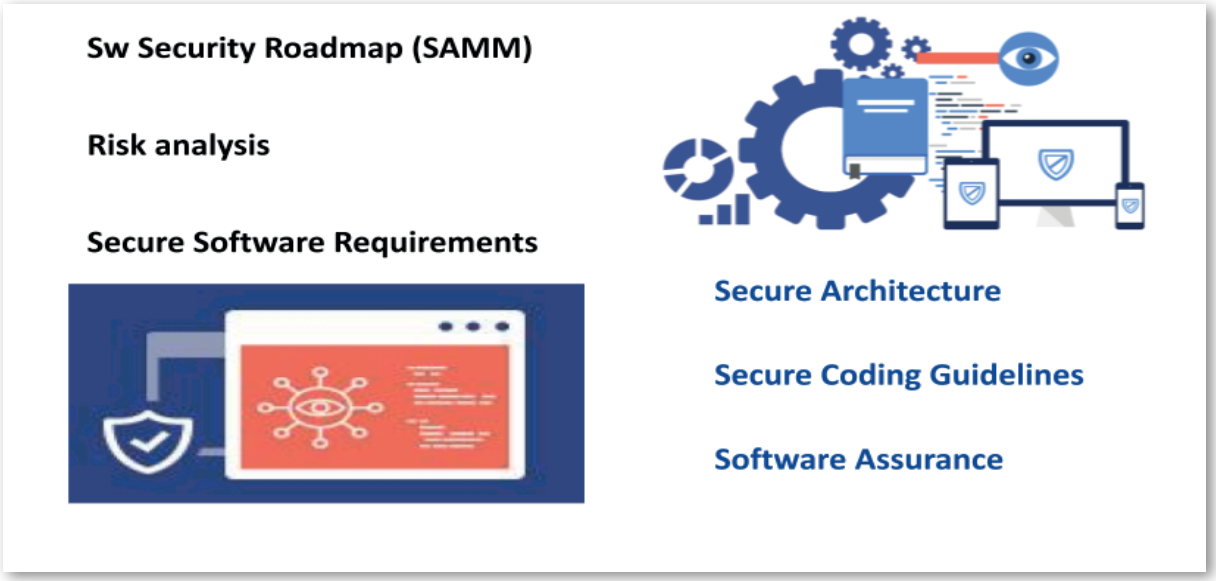


Figure: SwSec 5D Standards Dimension

The fifth dimension of the OWASP Software Security 5D Framework focuses on the implementation of standards related to software security. In order to effectively manage software security, companies need to have a solid understanding of the threats they face and the best practices to mitigate those threats. This dimension looks at the standards and practices that are in place to address software security concerns. Here are the standards that are analyzed as part of this dimension:

Sw Security Roadmap (SAMM)

The Software Assurance Maturity Model (SAMM) is a framework for building and improving software security programs. SAMM provides a set of guidelines and best practices that organizations can use to assess and improve their software security posture. The framework is divided into three areas: governance, construction, and verification. SAMM can be used as a roadmap for organizations to build and maintain secure software.

Risk analysis

Risk analysis is an important part of software security. It involves identifying and evaluating potential risks to the software and its data. A risk analysis should be performed for each project to identify and prioritize potential security risks. This analysis should consider the impact of the risk, the likelihood of the risk occurring, and the cost to mitigate the risk. The results of the risk analysis should be used to guide the implementation of security controls and to prioritize testing efforts.

Threat Modeling

Threat modeling is the process of identifying and prioritizing potential threats to a software system. The goal of threat modeling is to identify vulnerabilities in the software and to prioritize them based on their potential impact on the system. Threat modeling can be done at different stages of the software development lifecycle and should be performed whenever there are changes to the system or its environment.

Secure Architecture

Secure architecture is the design of software systems that are secure by design. Secure architecture should consider security at all levels of the system, including the network, application, and data layers. Secure architecture should also consider the potential threats to the system and should include appropriate security controls to mitigate those threats.

Secure Coding

Secure coding is the practice of writing code that is free from security vulnerabilities. Secure coding practices include following secure coding standards, using secure coding techniques, and testing code for security vulnerabilities. Secure coding should be integrated into the software development process to ensure that all code is secure by design.

Software Assurance

Software assurance is the process of ensuring that software is reliable, maintainable, and secure. Software assurance includes testing software for security vulnerabilities, patching software when vulnerabilities are discovered, and monitoring software for potential security issues. Software assurance should be part of the software development lifecycle and should be integrated into the software development process.

Overall, the fifth dimension of the OWASP Software Security 5D Framework provides a comprehensive view of the standards and practices that should be in place to ensure software security. By adopting these standards, organizations can build and maintain secure software that is resistant to potential threats and vulnerabilities. It is important for organizations to have a solid understanding of these standards and to integrate them into their software development process to ensure the security of their software systems.

In the next chaper we will focus on the survey.

3 | THE SURVEY

The SWSEC 5D survey is a tool designed to help organizations assess the maturity of their software security processes across the five dimensions of the SWSEC 5D framework. The survey consists of a series of questions that cover each of the five dimensions and is intended to be completed by individuals who are involved in the software development process, such as developers, security professionals, project managers, and executives.

The SWSEC 5D survey is a valuable tool for organizations that are looking to improve their software security posture. By completing the survey, organizations can gain a better understanding of their current level of maturity across the five dimensions of the SWSEC 5D framework. This information can then be used to identify areas where improvements can be made, and to develop a roadmap for improving the organization's software security processes.

The SWSEC 5D survey is typically administered by an independent third party, such as a consultant or a software security vendor. This helps to ensure that the results of the survey are objective and unbiased. The survey is usually administered online, and participants are typically given a set amount of time to complete the survey.

The SWSEC 5D survey consists of a series of questions that are designed to assess the maturity of the organization's software security processes across each of the five dimensions of the SWSEC 5D framework. For example, in the SwSec Processes dimension, questions may be asked about the organization's risk assessment process, its security requirements process, its threat modeling process, and its security design process.

In the SwSec Testing dimension, questions may be asked about the organization's adoption of security testing tools such as SAST, DAST, IAST, and RASP, as well as its use of external manual SCR and WAPT testing. In the SwSec Team dimension, questions may be asked about the roles and responsibilities of the organization's AppSec manager/CISO, security champions, AppSec specialists, satellite architects, satellite developers, and satellite auditors.

In the SwSec Awareness dimension, questions may be asked about the level of software security awareness among various roles within the organization, such as management, application owners, analysts, auditors, architects, developers, and engineers. Finally, in the SwSec Standards dimension, questions may be asked about the organization's adherence to software security standards such as the SW Security Roadmap (SAMM), risk analysis, threat modeling, secure architecture, secure coding, and software assurance.

Once the SWSEC 5D survey has been completed, the results are typically analyzed by the third-party consultant or vendor. The results are then presented to the organization in the form of a report, which typically includes a summary of the organization's current level of maturity across each of the five dimensions of the SWSEC 5D framework, as well as recommendations for improving the organization's software security processes.

Overall, the SWSEC 5D survey is a valuable tool for organizations that are looking to improve their software security posture. By assessing the organization's current level of maturity across each of the five dimensions of the SWSEC 5D framework, the survey can help organizations to identify areas where improvements can be made, and to develop a roadmap for improving their software security processes.

The following is the Google Form in ordet to access to the SwSec 5D Survey: https://docs.google.com/forms/d/e/1FAIpQLSej3Y32MUSnp0M5ngQXcuOyaQWAUNZ-A7VvrCy-3RX73qjLSA/viewform

The following figure shows a screenshot of the first page of the Survey:

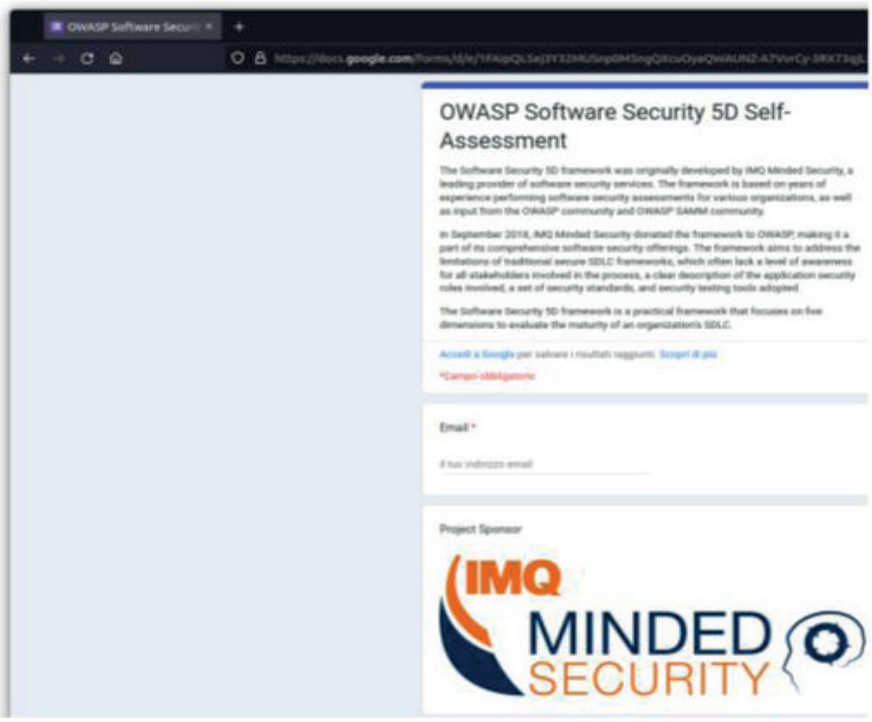


Figure: SwSec 5D Survey

The survey consists of the following set of questions for each of the 5 dimensions of the model. Each question will be evaluated with a value from 0 (no maturity) to 3 (complete maturity).

SWSEC PROCESSES

PR1. Are most of your applications and resources categorized by risk?

PR1 Evaluation:

- *A data and application risk classification system has been documented (3)*
- *Not at the moment (0)*
- *I do not know (0)*

PR2. Do you have security requirements with use case derived by the new vulnerabilities?

PR2 Evaluation:

- *Yes (3)*
- *No (0)*
- *I do not know (0)*

PR3. Do you review the architectures used in the projects before implement it?

PR3 Evaluation:

- *Yes (3)*
- *Sometimes (1)*
- *No (0)*
- *I do not know (0)*

PR4. Is your Company applying a threat modeling methodology for most of your new applications?

PR4 Evaluation:

- *Yes (3)*
- *No (0)*
- *A few (1)*
- *I do not know (0)*

PR5. Is your Company applying secure design patterns at the new sw projects?

PR5 Evaluation:

- *Yes (3)*
- *No (0)*
- *A few (1)*
- *I do not know (0)*

PR6. Are Secure Code Review and Web Application processes in place?

PR6 Evaluation:

- *Yes (3)*
- *No (0)*
- *For a few applications (1)*
- *I do not know (0)*

PR7. Do you have a Software Security Assurance process in place to avoid to have/buy not secure software?

PR7 Evaluation:

- *Yes (3)*
- *No (0)*
- *I do not know (0)*

PR8. Is the security bug fixing process in place and working well?

PR8 Evaluation:

- *Yes (3)*
- *No (0)*
- *Needs improvement (1)*
- *I do not know (0)*

PR9. Is a technology like WAF or RASP in place in order to monitor running web applications?

PR9 Evaluation:

- *Yes (3)*
- *No (0)*
- *Not for all the applications (1)*
- *I do not know (0)*
-

SWSEC TESTING

TE1. Do you implement automation to verify the security of your software? Please check the tool you are using: - SAST, DAST, IAST, RASP

TE1 Evaluation:

- *SAST (1)*
- *DAST (1)*
- *IAST (2)*
- *RASP (2)*

TE2. Does an external Company perform manual testing on your critical applications?

TE2 Evaluation:

- *No (0)*
- *Yes Manual Secure Code Review (SCR) (2)*
- *Yes Manual Web App Penetration Testing (WAPT) (1)*
- *Yes SCR and WAPT (3)*

SWSEC TEAM

TE1. Are the following figures present in your Company?

- CISO
- Application Security Manager
- Application Security Specialists

TE1 Evaluation:

- *nobody (0)*
- *1 (1)*
- *2 (2)*
- *3 (3)*

TE2. Do you think there is a person in the Security team that is able to follow software projects from the beginning to the end, verifying all the aspects of security?

TE2 Evaluation:

Yes (3)
No (0)
I do not know (0)

SWSEC AWARENESS

AW1. Is the management involved in workshops or seminars to be informed regarding Software Security risks?

AW1 evalutation:

- *Not yet (0)*
- *Yes, once a year (3)*
- *Yes, once every 5ys (1)*
- *I do not know (0)*

AW2. Are the business analyst trained on threat modeling?

AW2 evaluation:

- *Yes (3)*
- *No (0)*
- *I do not know (0)*

AW3. Are most roles in the development process given role-specific training and guidance?

AW3 evaluation:

- Role specific application security training is given to developers, architects, QA, *etc. (3)*
- *Only generic training (1)*
- *No at the moment (0)*

SWSEC STANDARDS

SS1. Is there a software security assurance program already in place?

SS1 Evaluation

- *Assurance program is documented and accessible to staff (3)*
- *Not at the moment (0)*
- *I dont know (0)*

SS2. Are secure coding guidelines in place? For all the languages used to develop software (such as J2EE, .Net, Android, iOS)?

SS2 Evaluation

- *Yes (3)*
- *No (0)*
- *I do not know (0)*

SS3. Do you apply security requirements into software supplier agreements?

SS3 Evaluation

- *Yes (3)*
- *No (0)*
- *I do not know (0)*

SS4. Are most of your applications and resources categorized by risk?

SS4 Evaluation

- *Yes (3)*
- *No (0)*
- *I do not know (0)*

SS5. Regarding third party code used in your applications, does the Company perform a security review before implementing it?

SS5 Evaluation

- *Yes (3)*
- *No (0)*
- *I do not know (0)*

SS6. Do you have a methodology in place to perform a Threat Modeling before the developing phase?

SS6 Evaluation

- *Yes but we do not use it (1)*
- *Yes and we use it (3)*
- *No (0)*
- *I do not know (0)*

SS7. Are project teams being audited for usage of secure architecture components?

SS7 Evaluation

- *Audits include evaluation of usage of recommended frameworks, design patterns, shared security services, and reference platforms (3)*
- *No (0)*
- *I do not know (0)*
- *In the following chapter we will identify the results and possible actions to implement in the roadmap.*

4 | THE DATA

The SwSec 5D Framework provides a comprehensive view of the company's software security practices, and the scorecard helps the company to identify the areas where it needs to improve. This way, the company can prioritize its efforts and resources to improve its software security practices in a structured and efficient way.

The SwSec 5D Framework provides a practical and comprehensive approach to evaluate the maturity of a company's software security practices. The scorecard enables the company to identify the areas where it needs to improve, and prioritize its efforts and resources to improve its software security practices. By implementing the recommendations provided by the SwSec 5D Framework, the company can enhance its software security practices, reduce the risk of security breaches, and increase the trust of its customers and stakeholders.

The following scorecard enlights what the assessed company is implementing today and what is missing. You can identify immediately the level of maturity for each dimension. Only 1 level has reached the right maturity. The Framework tells you that you MUST grow in all 5 dimensions in order to be mature.

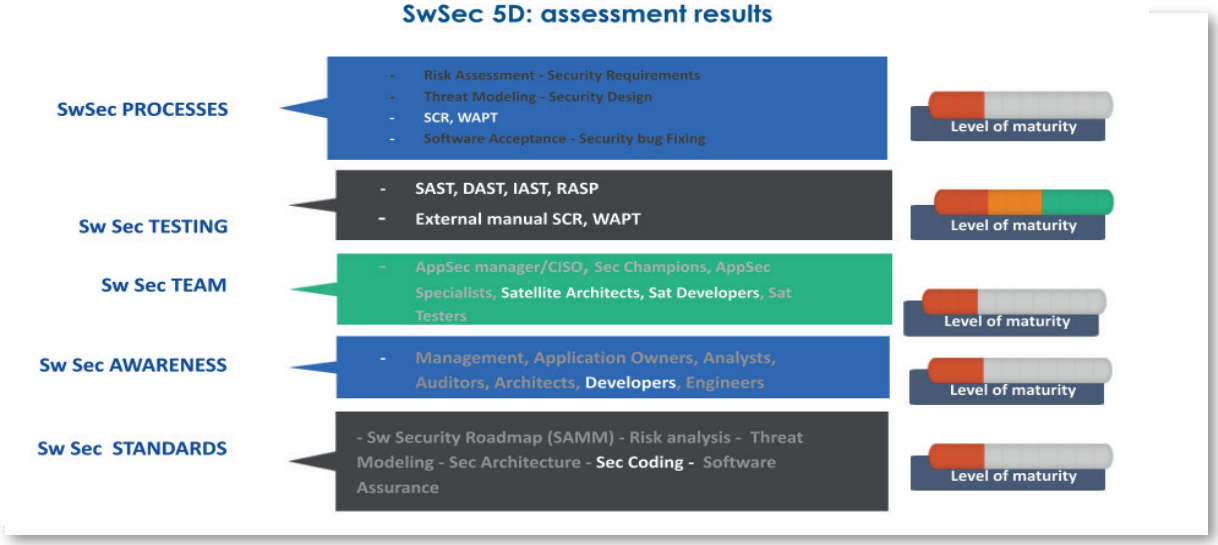
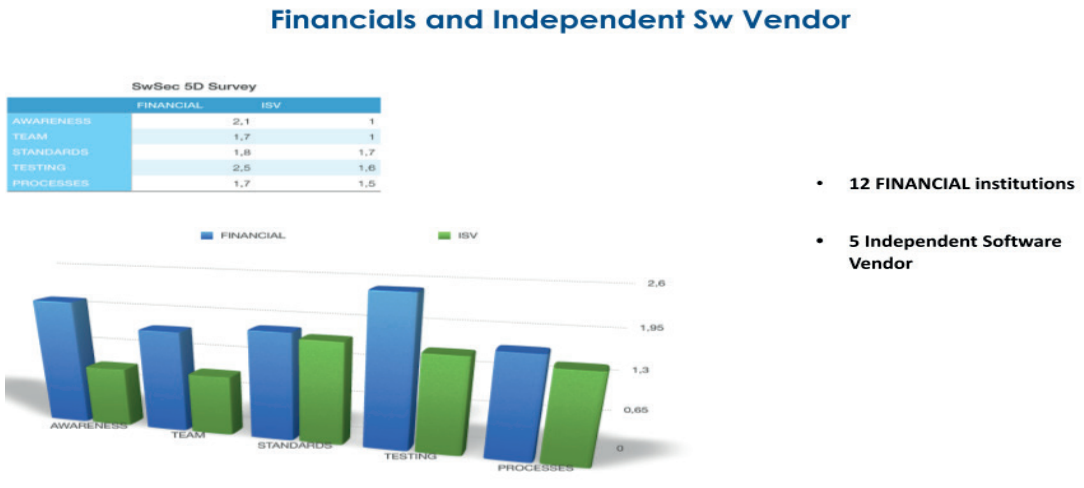


Figure: SwSec 5D Assessment Results

During our study, we conducted 17 assessments, analyzing 12 financial institutions and 5 independent software vendors. Our research aimed to provide insight into the current state of software security in the financial sector, highlighting areas for improvement and potential best practices. Through a rigorous evaluation of each organization's software security processes, testing, team, awareness, and standards, we were able to draw meaningful conclusions about the state of software security across the industry.



5 | ROADMAP & RESULTS

At the end of the assessment we can collect the results and given the set of activities to implement if the results are less then value 3.

SWSEC PROCESSES

- PR1 Implement a Risk Assessment process in order to categorize by risk your applications
- PR2 Security Requirements (standard use cases, new vulns)
- PR3 Implement a Security Architecture Process in order to have a Company standard of reviewed architectures
- PR4 Realizing the threat modeling methodology to be applied to projects valued at medium to high risk in the definition phase of the project;
- PR5 Secure Design
- PR6 SCR and WAPT standard are necessary to perform the security analysis following your internal standards
- PR7 Create a Software Assurance process to be sure that the development phase is following all your security requirements
- PR 8 implement a Security bug fixing process lead by satellite developers
-
- PR 9 Secure Monitoring using WAF or RASP technologies

SWSEC TESTING

- TS1 Utilize automated security testing tools for all the applications (DAST and IAST tools are preferred);
- TS2 Utilize automated secure code analysis tools for all the software (SAST and IAST tool are preferred).
- TS3 Utilize manual testing for high risk applications;
- TS4 Utilize manual secure code review during the development for high risk projects.

SWSEC TEAM

- TE1 Formalize the Security Manager role in order to strengthen the real role in the company. He must become the guarantor of the dissemination of culture on software security, and the focal point in your company for the adoption of standards and security processes in software development.
- TE2 Identify Security Champions or externalize this function

SWSEC AWARENESS

- AW1 Conduct security awareness training for all people involved in SDLC: half a day for managers, architects, developers, marketing
- AW2 Plan trainings for analysts: "Threat Modeling" (2 days);
- AW3 Trainings for developers: 'Building Secure Software for specific platforms' (2-5 days).

SWSEC STANDARDS

- SS1 Maintain a Software Security Roadmap using the OWASP SAMM model.
- SS2 Build and maintain secure coding guidelines for your developing environments; share the guidelines with development teams with training courses with final exam.
- SS3 Review security requirements into supplier agreements for the Governance of the Software

Security with the outsourcers

- SS4 Classify data and applications based on business risk.
- SS5 Maintain a list of recommended software frameworks to use in your projects.
- SS6 Explicitly apply security principles to design using a Threat Modeling standard.
- SS7 Establish formal Secure architectures and platforms standards.

RESULTS

The self-assessment in the OWASP SwSec 5D project provides a way for companies to evaluate their software security practices and identify areas for improvement. Once the assessment is completed, the results can be used to generate a report that highlights the company's level of maturity in each of the five dimensions.

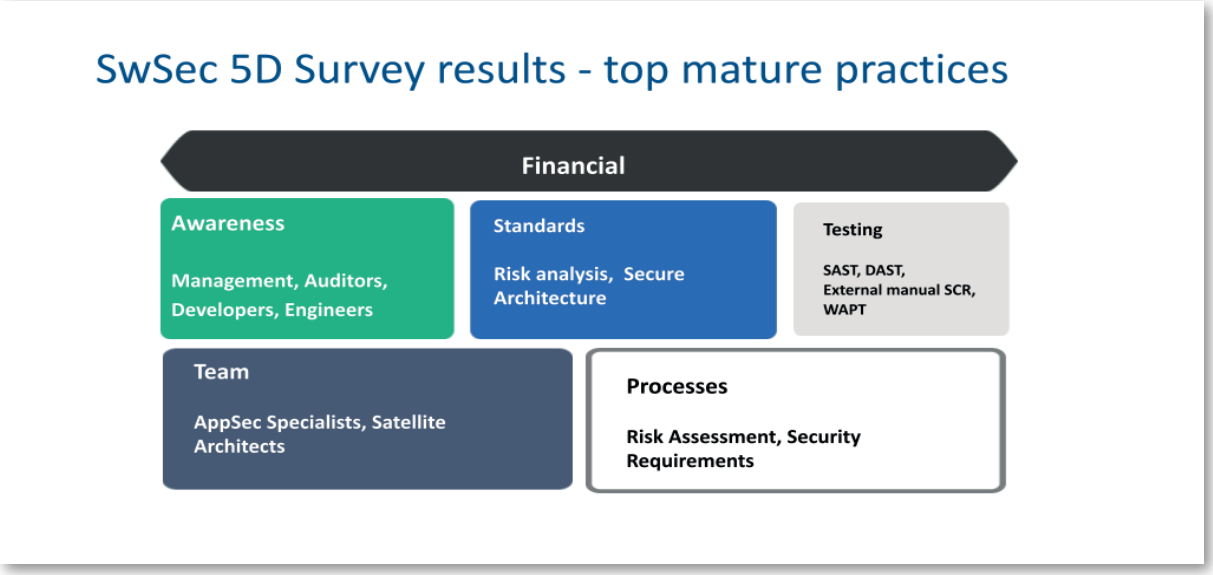
The report can provide valuable insights into the company's software security practices and identify areas where improvements can be made. For example, if the company scores low in the SwSec TESTING dimension, it may be an indication that they need to adopt more testing tools like SAST, DAST, IAST, or RASP, or perform more external manual SCR and WAPT testing. Alternatively, if the company scores low in the SwSec TEAM dimension, it may indicate that they need to establish more roles like AppSec manager/CISO, Sec Champions, AppSec Specialists, or Satellite Architects.

The report can also provide a comparison of the company's maturity level with other organizations that have completed the self-assessment. This can provide a benchmark for the company to compare its maturity level against industry standards and best practices. Additionally, the report can be used to communicate the current state of the company's software security practices to stakeholders, including management, customers, and partners.

In summary, the self-assessment in the OWASP SwSec 5D project provides a valuable tool for companies to evaluate their software security practices and identify areas for improvement. The results of the assessment can be used to generate a report that provides insights into the company's software security practices and can be used to compare against industry standards and best practices. The report can also be used to communicate the current state of the company's software security practices to stakeholders.

The following is an example of results:

Figure: SwSec 5D Assessment Report



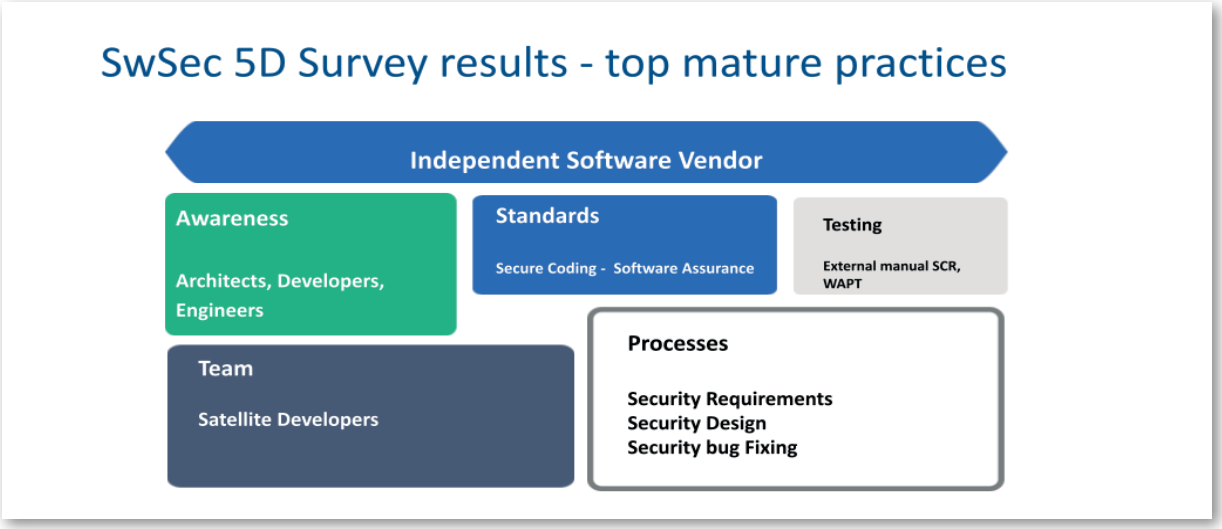


Figure: SwSec 5D Financial Top mature practices & SwSec 5D Independent Software Vendor practices

OWASP SAMM Assessment and 5D Framework are two important standards that help companies to develop their software security strategies. In this essay, we will explore both frameworks in detail and highlight their benefits and limitations.

One of the key benefits of the OWASP SAMM Assessment is that it provides a comprehensive view of software security. The framework covers all aspects of software security, from governance to deployment. This ensures that organizations have a complete understanding of their software security posture and can identify areas for improvement.

Another benefit of the OWASP SAMM Assessment is that it is adaptable to different types of organizations and software development lifecycles. The framework is designed to be flexible and can be customized to meet the unique needs of each organization. This allows organizations to develop a software security strategy that is tailored to their specific needs.

However, the OWASP SAMM Assessment also has some limitations. One limitation is that it can be time-consuming and resource-intensive to complete. The framework requires organizations to conduct a detailed analysis of their software security practices, which can be a significant undertaking. Additionally, the framework does not provide guidance on how to implement the recommended activities, which can be challenging for organizations that are new to software security.

The OWASP 5D Framework is a comprehensive framework that focuses on five dimensions of software security: Processes, Testing, Team, Awareness, and Standards. The framework is designed to provide a practical approach to software security that is easy to implement and understand. The 5D Framework is based on the principle that software security is not just the responsibility of the security team but of everyone involved in the software development process.

The 5D Framework includes a detailed checklist of activities for each dimension of software security. The checklist includes both qualitative and quantitative measures, which allows organizations to measure their progress over time. The framework is designed to be flexible and adaptable to different types of organizations and software development lifecycles.

However, the 5D Framework also has some limitations. One limitation is that it may not be as comprehensive as other frameworks, such as the OWASP SAMM Assessment. The framework focuses on five dimensions of software security, while other frameworks may cover a broader range of topics. Additionally, the framework may not be suitable for organizations with more complex software development lifecycles or security requirements.

The OWASP 5D framework was designed to help companies understand the need to grow in all five dimensions simultaneously, rather than focusing on just one or two. In order to be considered mature, a company must be mature in all five dimensions.

OWASP®

owasp.org