Universität Regensburg

Policy

Compliance Framework Policy

Responsible process	Master Thesis
Process owner	Lehner Maximilian
Author / Company	Lehner Maximilian
Version created on	2025-01-15
Document ID / Version	DM00xxxx / 1.0
Text Revision	60

Table of Contents

1 Version Index 3
2 Approval Matrix 3
3 Purpose 3
4 Scope 3
5 OWASP SAMM 4
6 Relevant Stakeholders 5
7 Standards and Regulations 5
8 Security Levels and Abstract Warehouse Model 6
9 Integration with the Compliance Framework 8
10 Dynamic Nature of the Policy 8
11 Terms and Abbreviations 9

Universität Regensburg

List of Tables

1 Table: References 9
2 Table: Terms and Abbreviations 9

List of Figures

1 Differentiation between IT and OT approaches. 3
2 OWASP SAMM overview. 4
3 Using OWASP SAMM as a foundation for achieving Maturity Level 1. 5
4 OWASP ISVS overview. 6
5 Abstract Model of a Smart Warehouse. 7

1 Version Index

The following modifications were made compared to the previous version:

Version	Description	Date	Responsible
1.0	Created the document	2025-01-15	Lehner Maximilian

2 Approval Matrix

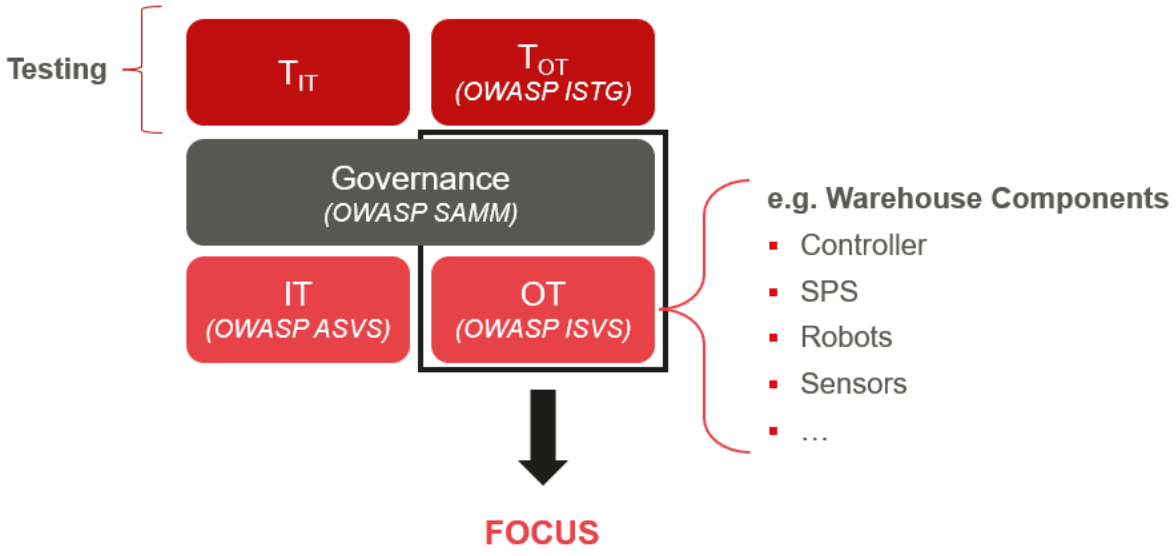
Abbreviation	Role	Date	Signature

3 Purpose

This policy defines the principles, guidelines, and responsibilities for ensuring cybersecurity compliance in IIoT environments. It provides a structured framework to address the specific challenges of securing OT systems while aligning with recognized industry standards and regulations. By implementing this policy, organizations can protect their IIoT assets, maintain operational continuity, and demonstrate adherence to security best practices.

4 Scope

The policy applies to all IIoT systems, including Cloud, IT, and OT components, within the operational environment. Traditional IT systems are included only when they directly interact with IIoT components. A visual representation of this scope, emphasizing the focus on OT systems, is provided in the figure below (Figure 1). This ensures clarity on the boundaries of the policy and its applicability.

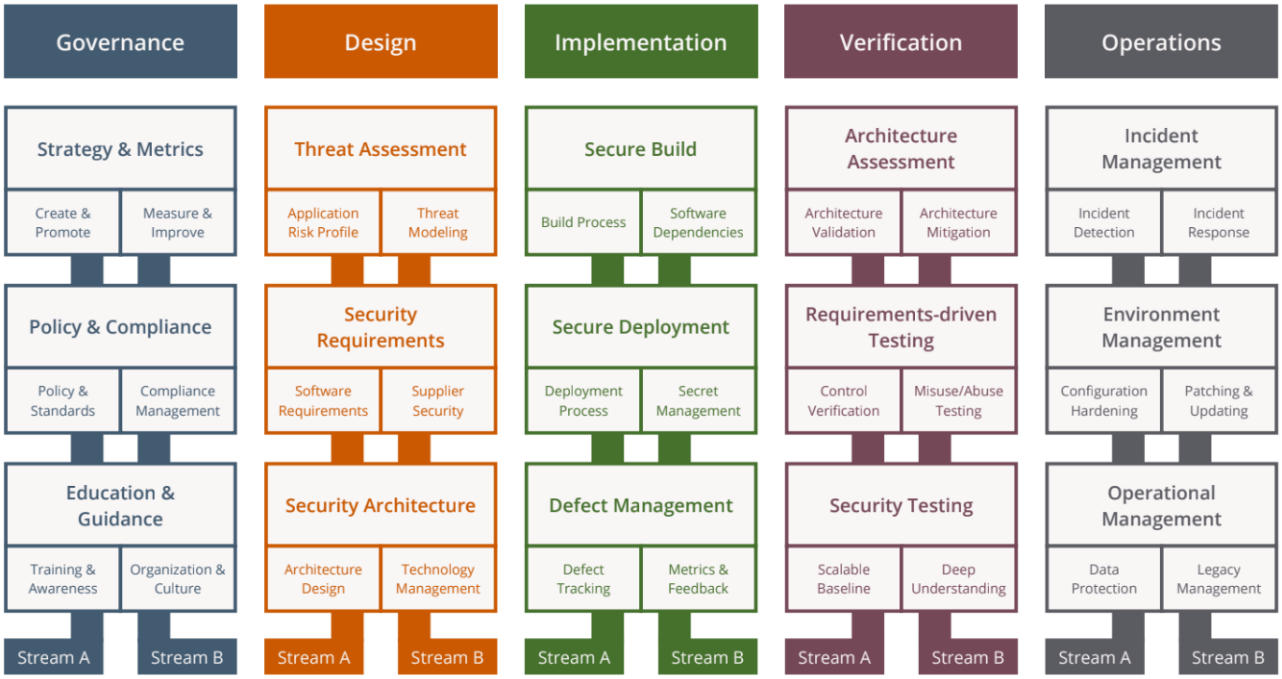


1 Differentiation between IT and OT approaches.

5 OWASP SAMM

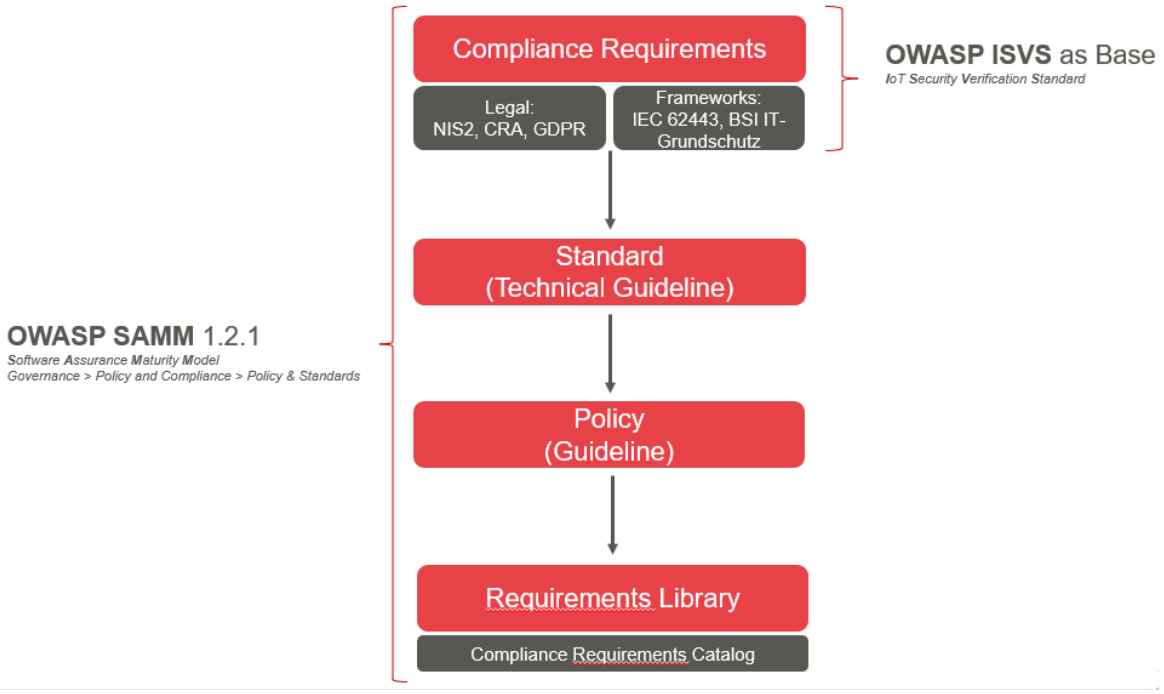
The Software Assurance Maturity Model (SAMM) serves as the overarching framework for structuring the compliance framework. OWASP SAMM provides a structured approach to achieving software security maturity by aligning security practices with organizational goals.

This compliance framework enables organizations to meet **Maturity Level 1** under **OWASP SAMM 1.2.1**, specifically in the domain of "Policy & Compliance → Policy & Standards" under "Governance." This level establishes foundational practices such as the definition of policies and standards, which are essential for effective cybersecurity management. A visual overview of the OWASP SAMM framework is provided in Figure 2.[1]



2 OWASP SAMM overview.
[1]

By integrating OWASP SAMM into the compliance framework, the policy ensures that the organization's security practices are systematically aligned with recognized maturity models, as illustrated in the Figure 3. This alignment also responds to customer requirements, as organizations like TGW Logistics Group often face inquiries about their maturity levels under OWASP SAMM.



3 Using OWASP SAMM as a foundation for achieving Maturity Level 1.

6 Relevant Stakeholders

This policy is designed for the following key stakeholders:

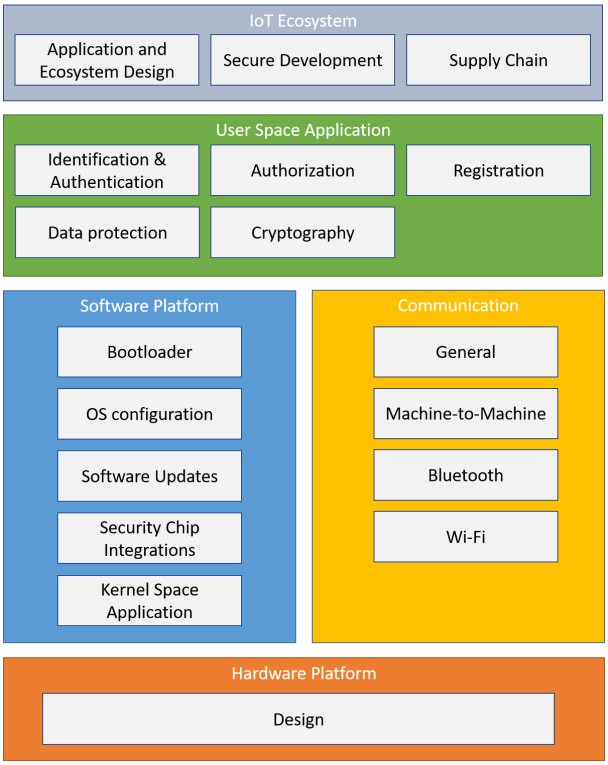
- **OT Security Teams**: Responsible for safeguarding operational technology and ensuring compliance with security measures.
- **IT Security Teams**: Ensure secure interaction between IT and OT systems and manage overall data integrity.
- **Compliance Officers**: Oversee adherence to regulatory requirements and alignment with industry standards.
- **Management**: Ensure resource allocation and support for implementing the compliance framework.
- **System Administrators**: Implement technical controls and maintain compliance with specified requirements.

7 Standards and Regulations

This policy incorporates requirements from the following standards and regulations:

- **OWASP ISVS**: Provides the foundational structure for organizing and categorizing security requirements into three security levels (1, 2, and 3). Its structured and well-documented format serves as the baseline for the framework. A visual representation of the OWASP ISVS structure is shown in Figure 4.[2]
- **IEC 62443**: Specifically, IEC 62443-3-3 was used to address OT security requirements for system-level operations, while IEC 62443-4-2 was indirectly included as it is referenced extensively by the CRA. These standards are widely recognized in the EU and provide granular, actionable security measures.[3] [4]

- **Cyber Resilience Act (CRA)**: The CRA's requirements, as outlined in **TR-03183-01**, address regulatory obligations for securing IIoT environments. TR-03183-01 provides specific, actionable guidelines that complement the broader objectives of the CRA. Its integration ensures alignment with EU regulations and enhances the framework's relevance to regulatory contexts.[5]



4 OWASP ISVS overview. [2]

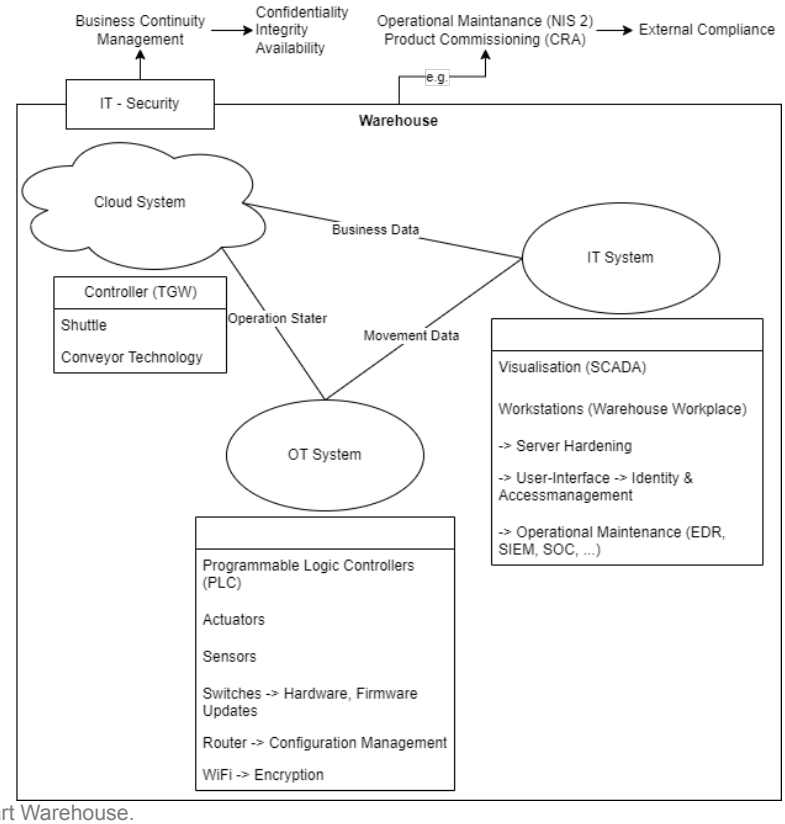
8 Security Levels and Abstract Warehouse Model

The policy adopts the OWASP ISVS security levels to classify compliance requirements:

- **Level 1**:
  The goal of level one requirements is to provide protection against attacks that target software only, i.e. attacks that do not involve physical access to the device. Level one requirements aim to provide a security baseline for connected devices where physical compromise of the device does not result in high security impact. These are devices where the device's IP should not be protected, where no sensitive information is being stored on the device, and where compromise of one device does not allow an attacker to move laterally to other devices or systems on the IoT ecosystem.
  An example of a level one device is a smart light bulb created with off the shelf hardware and software components. Compromise of the light bulb would not result in an attacker gaining access to state-of-the art technology. If no personal data is stored on the device, there is no data to be stolen. If authentication and authorization are correctly implemented on the supporting cloud infrastructure, the worst thing the attacker could do is spoof the status of the compromised light bulb.[2]

- **Level 2**:
  The goal of level two requirements is to provide protection against attacks that go beyond software and that target the hardware of the device. Devices that adhere to level two requirements are devices where compromise of the device should be avoided. These are devices where the device's IP should be protected to a reasonable extent and where there is some form of sensitive information stored on the device.
  Examples of level two devices are smart locks, alarm systems, smart cameras, and medical devices that aggregate measurement data and send it to a physician for analysis.[2]
- **Level 3**:
  The goal of level three requirements is to provide requirements for devices where compromise should be avoided at all cost. Devices where there is highly sensitive information stored on the device or where compromise of the device can result in fraud. In addition to the security requirements provide by level one and two, level three requirements focus on defense-in-depth techniques that attempt to hinder reverse engineering and physical tampering efforts.
  Examples of level three devices consist of hardware crypto wallets, smart-meters, connected vehicles, medical implants, recycle machines that trade aluminium cans for money.[2]

As an example, the abstract warehouse model (Figure 5) demonstrates how these levels are applied to Cloud, IT, and OT components within a smart warehouse. Cloud and IT systems are classified as Level 2, reflecting their need for robust but moderate security measures. OT systems are typically Level 2 but may require Level 3 compliance when classified as critical infrastructure under KRITIS.



5 Abstract Model of a Smart Warehouse.

9 Integration with the Compliance Framework

This policy is tightly integrated with the compliance framework, leveraging the **Compliance Requirements Catalog** and the **Compliance Questionnaire** to operationalize its principles. The catalog provides a comprehensive set of requirements derived from the standards and regulations mentioned above, while the questionnaire serves as a practical tool for assessing the organization's compliance status.

The documents are accessible via the following links: Compliance Requirements Catalogue, Compliance Questionaire

10 Dynamic Nature of the Policy

The policy is designed to remain adaptable to evolving standards and regulations. Changes to the Compliance Requirements Catalog or Questionnaire are automatically reflected in the policy, ensuring its continued relevance without requiring extensive revisions.

References

Reference-ID	Description/Link
1	OWASP SAMM Model (https://owaspsamm.org/model/)
2	OWASP ISVS Github (https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS/)
3	ISA/IEC 62443 Official Website (https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards/)
4	Quick Start Guide: An Overview of ISA/IEC 62443 Standards (https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf)
5	BSI TR-03183-01 (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html/)

1 Table: References

11 Terms and Abbreviations

Term/Abbreviation	Description
IIoT	Industrial Internet of Things
OT	Operational Technology
CRA	Cyber Resilience Act
TR-03183-01	Technical Guideline for CRA compliance
OWASP ISVS	Open Web Application Security Project Internet of Secure Things Verification Standard
OWASP SAMM	Open Web Application Security Project Software Assurance Maturity Model
IEC 62443	International standards for securing OT systems

2 Table: Terms and Abbreviations