Axis Security Development Model

Introduction

Axis commitment to secure development

It's mandatory for all Axis development teams to adhere to the Axis Security Development Model (ASDM). ASDM is a framework that defines the process and tools used by Axis to build software with security built-in throughout the lifecycle, from inception to decommission.

ASDM objectives

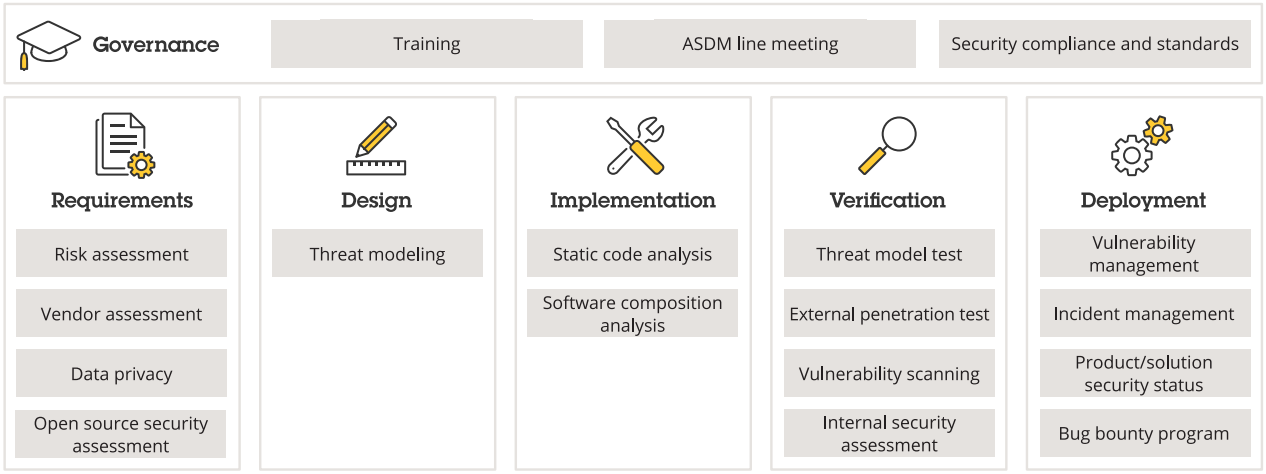
The primary objectives driving ASDM efforts are:

- Making software security an integrated part of Axis software development activities.
- Reducing security related business risks for Axis customers.
- Meeting increasing awareness of security considerations by customers and partners.
- Creating potential for cost reduction because of early detection and resolution of issues

The scope of ASDM is software included in Axis products and solutions.

ASDM overview

The ASDM consists of several activities spread across the development lifecycle. The security activities are collectively identified as the ASDM. The latest version is 2024.02, seen below.



The Software Security Group (SSG) is responsible for governing the ASDM and evolving the toolbox over time. There is an ASDM roadmap and a rollout plan for implementing activities and increasing ASDM maturity across the development organization. Both the roadmap and rollout plan are owned by the SSG, but the responsibility for actual implementation in practice, such as activities related to development lifecycle, is delegated to the development teams.

Giving the team ownership of ASDM and its implementation means that the manager is responsible for the adoption of activities. Instead of a setup where the SSG pushes a central ASDM rollout plan, it now becomes pull-based and controlled by the managers.

Software Security Group (SSG)

The SSG is responsible for facilitating secure development practices and fostering a security culture in the organization. The group consists of security coaches who are responsible for development and maintenance of the ASDM as well as coaching satellites and teams to ensure security is built-in during development. The SSG is the main internal contact entity towards the development organization for security-related issues.

The reasons for having SSG are to:

- Ensure a structured approach to improving the security of Axis products and solutions
- Ensure that the ASDM works for all Axis-branded products and solutions
- Coordinate the ASDM usage across development teams
- Make the ASDM status known and transparent
- Facilitate knowledge sharing, including best practices

Satellites

Satellites are members of the development organization that spend a part of their time driving work with software security aspects. The reasons for having satellites are to:

- Scale ASDM without building a large central SSG
- Provide ASDM support close to the development teams
- Facilitate knowledge sharing, including best practices

A satellite will assist in implementing new activities and maintaining the ASDM in a subset of the development teams.

Roles and responsibilities

As shown in in the table below, there are some key entities and roles which are part of the ASDM. The table below summarizes roles and responsibilities in relation to the ASDM.

Role/Entity	Part of	Responsibility	Comment
Security coach	SSG	Govern and evolve ASDM. Coach satellites and teams on how to use ASDM, and coach managers to use ASDM status to drive their organization.	100% assigned to SSG
Satellite	Development line	Assist SSG in implementing ASDM, coach teams, perform trainings and ensure that the team can continue to use the toolbox as part of the daily work, independently from SSG.	Interested and committed developers, architects, testers, and similar roles who have a natural affinity for software security. Satellites assign at least 20% of their time to ASDM related work. Cross-team responsibility (several teams) required to constrain total number of satellites.
Managers	Development line	Secure resources for implementation of ASDM practices. Drive tracking and reporting on ASDM progress and coverage. Ensure teams are trained and that there is satellite coverage.	Security is something that has to be prioritized by managers to ensure software is developed with security in mind. Managers refer to both line managers and directors.
Development teams	Development line	Use the tools in ASDM with help from satellites and SSG.	The development team consists of people that work with development of software in any way for example developers and testers. Testers are independent from developers and the development organisation.
Product security team	Product management	Handle external communication for incident and vulnerability management and drive work on security features.	Product management consists of product owners and product specialists.
AXIS OS R&D Steering Group and CTO	R&D management	Decides on security strategy and acts as main SSG stakeholder.	SSG reports status and ASDM roadmap to AXIS OS R&D Steering Group and CTO on a regular basis.

ASDM activity rollout

ASDM activity rollout to a development team is a staged process:

1. The team is introduced to the new activity through training.
2. The SSG works together with the team to perform the activity, like risk assessment or threat modeling, for selected parts of the system(s) managed by the team.
3. Further activities related to integrating the toolbox in the team's workflow will be handed over to the manager, team and satellite when they are ready to work independently without direct SSG involvement.

The rollout is repeated when there are new versions of the ASDM available with modified and/or added activities. The amount of time spent by the SSG with a team is highly dependent on the activity and code complexity. A key factor for successful handover to the team is the existence of a satellite who can continue further ASDM work with the team. The SSG drives learning and assignment of the satellite in parallel with activity rollout.

The figure below summarizes the rollout methodology.

The SSG's definition of "done" for handover is:

- Training performed
- Satellite assigned
- Team is ready to perform the ASDM activity
- A regular ASDM status meeting with line and QA managers, satellites and SSG members is established

The SSG uses input from the teams to prepare status reports for senior management.

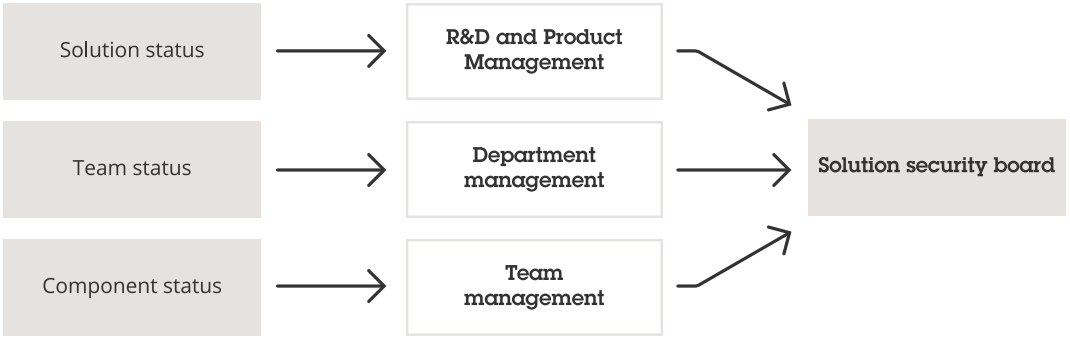
ASDM governance

ASDM status structure

The ASDM status structure has two perspectives: one team-centric, mimicking our team and department structure with focus on the components made by the team, and one solution-centric, focusing on the solutions we bring to the market. Both of these perspectives are essential to keep the model alive and ensure security work is being done.

To verify the security posture in the organization, these two perspectives come together in a solution security board consisting of different R&D managers. It is the responsibility of the managers to ensure that there is a security status to be reported to the board.

The figure below illustrates the ASDM status structure.



Component status

We have a broad definition of component, since we need to cover all sorts of architectural entities ranging from Linux demons in the platform, server software, and cloud services. Each team should have a clear view of all their high-risk components, including both new and legacy components. For solutions, we want to have insights into the security status of all their parts.

First, we need to know whether the component has undergone security analysis in order to determine if its security posture is known or unknown. To ensure that, each component is categorized according to its security analysis coverage as done, not done, or ongoing.

The metrics we use to capture the security quality of the component are based on the security work items in the backlog that are linked to the component. This could include countermeasures that have not been implemented, test cases that have not been executed, and security bugs that have not been addressed.

Component coverage is a part of the ASDM line meeting activity.

Team status

The team's status includes its assessment of its ASDM proficiency, metrics related to their security analysis activities, and an aggregation of the security status of the components they are responsible for. All of this is discussed during the ASDM line meetings.

The team's maturity is linked to which activities the team is performing. A team just starting out with ASDM would be expected to perform few activities, whereas teams that are proficient in their security work are expected to perform more activities and give feedback to the model.

Solution status

Solution status aggregates security status for a set of components that make up the solution.

The first part of the solution status is the analysis coverage of the components. This helps solution owners understand whether the security status of the solution is known or unknown. In one perspective it helps identify the blind spots.

The rest of the solution status contains metrics that capture the security quality of the solution. We do that by looking at the security work items that are linked to the components in the solution.

An important aspect of the security status is the bug bar defined by the solution owners. The solution owners must define an appropriate security level for their solution. For example, this means that the solution should have no outstanding critical or high severity work items open when released to the market.

This is covered in the ASDM product/solution security status activity.

ASDM activities

Training

Everyone that works with developing software at Axis should be empowered to do so. One aspect of empowerment is possessing the necessary degree of knowledge. The goal of training is to emphasize the importance of security, promote decentralized ownership, and inform people about ASDM activities and responsibilities that come with developing software at Axis.

These trainings range from digital courses to discussion-based sessions.

ASDM line meeting

The purpose of having regular follow-up meetings is to provide an essential feedback loop in a continuous improvement process. Managers, satellites, and the SSG meet and discuss the following topics at these meetings:

- Organizational capabilities to handle ASDM
- Execution of ASDM activities
- Component security status

ASDM assessment

The effectiveness of the ASDM model and its individual activities are evaluated on a regular basis. The aim is to identify gaps in activities, methods, and tools. The assessment relies on feedback from external sources via external penetration tests and bug bounty programs, but also from internal retrospectives.

Security compliance and standards

The goal is that development teams should only have to follow ASDM. Accordingly, the SSG performs regular evaluations of different security-related standards and maps them to ASDM. This is used as (one of many) inputs to the continuous evaluation and improvement of ASDM.

Risk assessment

A key ASDM objective is to optimize the efficiency of security activities within the teams to avoid slowing down development. Risk assessment is the fundamental method to determine the appropriate level of security effort based on contextual factors and inherent risk associated with new or old code.

Risk assessment entails judging whether a new product or added/modified feature in existing products increases risk exposure. Note that this also includes data privacy aspects and compliance requirements. Examples of changes that have a risk impact are new APIs, changes to authorization requirements, and new middleware

Vendor assessment

When Axis buys code (or products that include code) from vendors for the purpose of using it in Axis-branded products, we need to assess how the vendors conduct their security activities. Vendor assessment serves as a tool to comprehend their existing security practices, pinpoint areas for improvement, and advocate for the integration of security activities into their development processes.

Things Axis considers when assessing third-party software suppliers:

- The impact to the Axis brand if the third-party code has vulnerabilities that are exploited
- Development environment/IT security
- Secure software development activities
- Vulnerability and incident management

Data privacy

Trust is a key focus area for Axis and, as such, it is important to follow best practices when working with private data collected by our products, solutions and services.

The scope for Axis efforts related to data privacy are defined such that we can:

- Fulfill legal obligations
- Fulfill contractual obligations
- Help customers fulfill their obligations

We divide the **data privacy** activity into two sub-activities:

- Data privacy assessment
  - Done during **risk assessment**
  - Identifies if data privacy analysis is needed
- Data privacy analysis
  - Done, when applicable, during **threat modeling**
  - Identifies personal data and threats to personal data
  - Defines privacy requirements

Open source security assessment

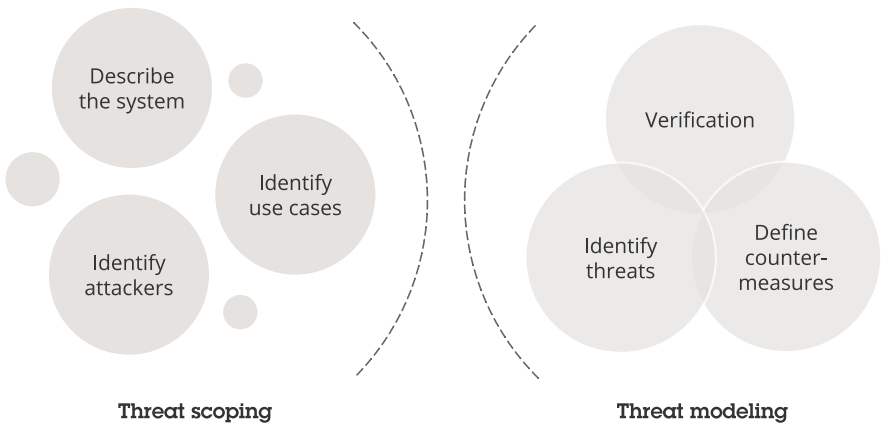
Open source security assessment refers to assessing how an open source project conducts security activities as well as defining a strategy to mitigate potential risks associated with the project. Third-party software risks can have a direct impact on the applications and systems that rely on it.

Things that Axis considers when assessing open source software components before use:

- Contributors
- Cadence of updates
- Vulnerability management

Threat modeling

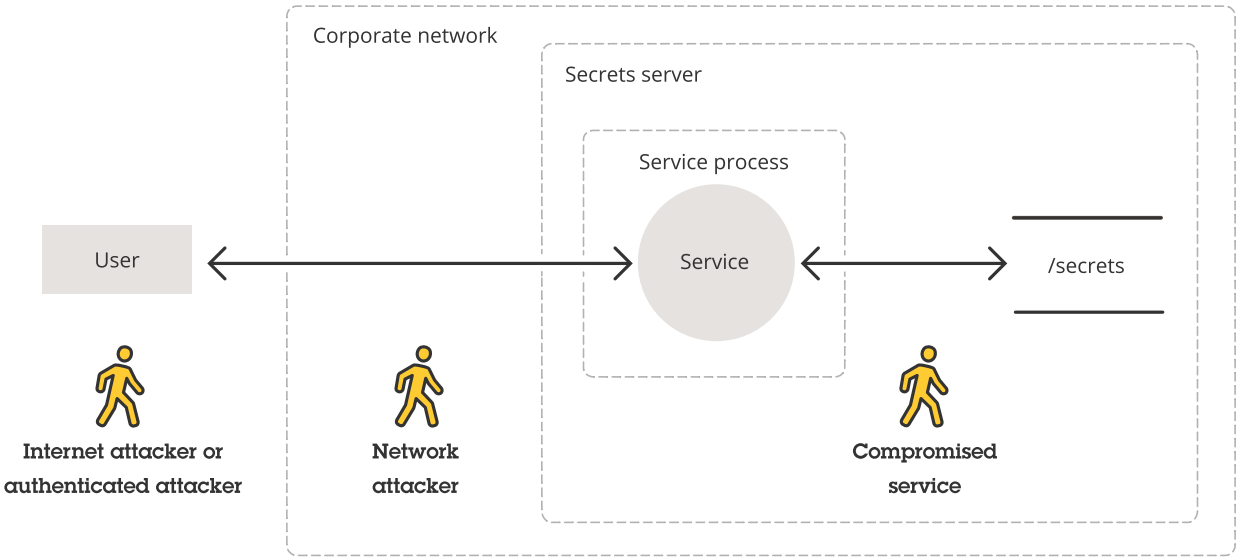
Threat modeling is a systematic approach to identify threats, define countermeasures, and plan verification early in the development process. However, before identifying threats, we need to decide on the scope of the threat model. A way of articulating the scope is to describe the attackers we need to consider. This approach will also allow us to identify the high-level attack surfaces we must include in the analysis.



The focus during threat scoping is on finding and categorizing attackers we want to handle using a high-level description of the system. Preferably, the description is visualized as a data flow diagram (DFD) since it makes it easier to relate the more detailed use case descriptions that are used when creating the threat model.

This does not mean that all the attackers we identify need to be considered. It simply means that we are explicit and consistent in relation to the attackers we will address in the threat model. Essentially, the attackers we choose to consider will define the security level of the system we are assessing.

Note that our attacker description does not factor in attacker capabilities or motivation. We have chosen this approach to simplify and streamline threat modeling as much as possible.



Threat modeling has three steps that can be iterated as the team sees fit:

1. Describe the system using a set of DFDs
2. Use the DFDs to identify threats and describe them in an abuse-case style
3. Define countermeasures for the threats and verification if the countermeasures

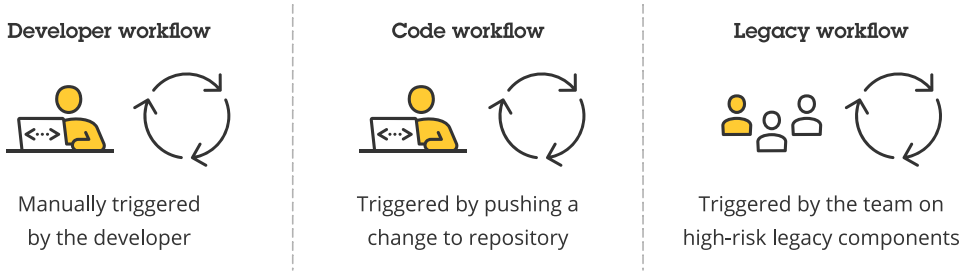
The result of a threat modeling activity is a threat model that contains prioritized threats and countermeasures. Development work required to address countermeasures is managed by creation of tickets both for the implementation and verification of the countermeasure. Teams can also have their threat model subjected to review.

Static code analysis

Static code analysis offers automated detection of some security bugs classes, reducing manual code review workload.

In the ASDM, teams can use static code analysis in three ways:

- Developer workflow: developers analyze the code they are working on
- Code workflow: developers get feedback in code review system
- Legacy workflow: teams analyze high risk legacy components



Software composition analysis

Software composition analysis identifies open source components within a software system and provides a continuous process to detect known security vulnerabilities associated with these components, ensuring proactive mitigation. Open and transparent communication regarding the components used and their associated vulnerabilities is crucial in order to fosters trust and transparency. All Axis software is provided with a software bill of material.

Threat model testing

Creating tests based on a threat model involves developing specific test cases to verify the effectiveness of countermeasures and assess the system's ability to withstand potential attacks. To emphasize the importance of verifying countermeasures, threat model testing is treated as a separate activity although it takes place in combination with threat modeling.

External penetration testing

In select cases, third-party penetration testing is performed on Axis hardware or software products. The main purpose of running these tests is to provide insight and assurance regarding the security of the platform at a particular time-point and for a particular scope.

One of our primary goals with the ASDM is transparency, and we encourage our customers to perform external penetration testing on our products. We are happy to collaborate when defining appropriate parameters for testing as well as discussions around interpreting the results.

All vulnerabilities found via external penetration testing receive CVE IDs and are thus publicly shared.

Vulnerability scanning

Regular vulnerability scanning allows the development teams to identify and patch software vulnerabilities before products are released to the public, reducing the customer's risk when deploying the product or service. Scanning is performed prior to each release (hardware, software) or on a running schedule (services) using both open-source and commercial vulnerability scanning packages.

The scan results are used to generate tickets in the bug tracking platform and marked with a distinct tag for prioritization by development teams. All vulnerability scans and tickets are stored centrally for traceability and auditing purposes.

Critical vulnerabilities should be resolved prior to release or in a special service release with other, non-critical vulnerabilities, tracked and resolved in alignment with the software release cycle. For more information on how vulnerabilities are scored and managed, see .

Internal security assessment

The purpose of an internal security assessment is to give feedback to teams about their security work and spread knowledge about security through target efforts. It is a deeper security test that is normally performed in the team. This activity is not conducted by the team itself but with person or persons outside the team to get another view on the component or system under assessment.

The results from an internal security assessment are used as input to:

- Improve the security level of the component or system under assessment
- Provide feedback on the effectiveness of the team's ASDM activities
- Provide feedback to the SSG on possible improvements to the ASDM
- Provide feedback on the internal security assessment methodology

Vulnerability management

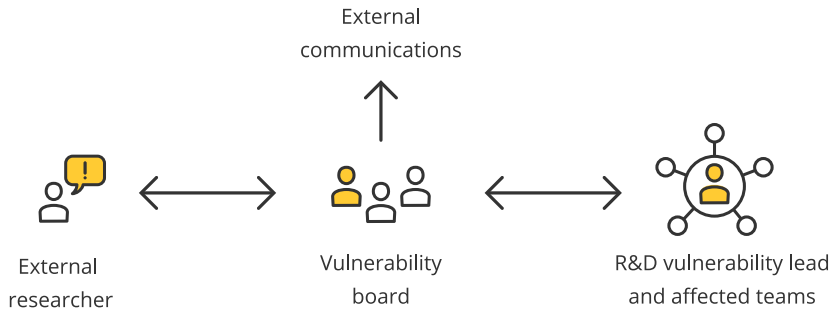
Axis is, since 2021, a registered CVE naming authority (CNA) and therefore capable of publishing standard CVE reports to the MITRE database for consumption by third-party vulnerability scanners and other tools.

The vulnerability board is the internal Axis contact point for vulnerabilities discovered by external researchers. Reporting of discovered vulnerabilities and subsequent remediation plans are communicated via the email address.

The main responsibility of the vulnerability board is to analyze and prioritize reported vulnerabilities from a business perspective, based on:

- Technical classification provided by the SSG
- Potential risk for end-users in the environment in which the Axis device operates
- Availability of compensating security controls (alternative risk mitigation without patching)

The vulnerability board registers the CVE number and works with the reporter to assign a Common Vulnerability Scoring System (CVSS) score to the vulnerability. The vulnerability board also drives external communication to partners and customers through Axis security notification service, press releases, and news articles. Read more in *Axis vulnerability management policy.*



Incident management

An incident is a weakness in a system that is being exploited. The organized approach to address and manage an incident is referred to as incident management. The goal of incident management is not just to provide a solution but to handle the situation in a way that limits damage and reduces recovery time and costs. Incident management is different from vulnerability management since there may be an active attacker that is inside the system.

Teams have their own playbook to manage incidents. The purpose of a playbook is to have a documented way to respond to and resolve an incident in a timely manner. Having a playbook empowers teams to take decisions during an incident but also serves as a reminder that incident management goes beyond the incident itself.

Product/solution security status

Integrating security into the release workflow involves everyone contributing to release decisions, such as project managers, product managers, QA, and development managers. Additionally, satellites and SSG members can participate in an advisory capacity to help with security considerations in the release process.

By regularly having discussions about the security status of a product or solution, we:

- Make informed decisions about the security of our products and solutions
- Make sure that the development line and product management is aligned on the security posture of our products and solutions
- Make sure that we have a complete and transparent view of the security status

Bug bounty program

The bug bounty program refers to a crowdsourced setup encouraging independent security researchers to discover and report vulnerabilities in Axis products. This activity is utilized by mature teams seeking external feedback on their ASDM efforts.

The bug bounty program reinforces Axis efforts to proactively identify, patch, and disclose vulnerabilities. All vulnerabilities found via the bug bounty program receive CVE IDs and are thus publicly shared.

ASDM activities history

ASDM was created using common best practices, but *specifically adjusted to the specific context of Axis Communications,* such as the company culture and product portfolio. Accordingly, Axis can adjust and optimize ASDM to our context, as opposed to following an already established security development lifecycle or standard from a different industry.

The original ASDM version (2018.01) consisted, by design, of few activities. As development teams at Axis have become more mature in their security work, more activities have been added. Some activities have evolved, particularly those with limited focus. As the teams and organization continued to mature, the SSG expanded the activities. A few activities have received a name change to signal more clearly what they entail.

Axis has defined the following ASDM versions.

ASDM version	Activities
2018.01	Added awareness training, role specific training, status follow up, risk assessment, 3rd party assessment, threat modeling, threat model code review, threat model testing, and vulnerability management.
2018.11	Added static code analysis.
2019.05	Added data privacy and ASDM assessment.
2019.12	Added software composition analysis.
2020.04	Added external pen-test.
2021.07	Added vulnerability scanning, firedrill and product/solution security status.
2022.02	Added ASDM audit.
2022.05	Added open source security assessment.
2022.10	Added bug bounty program. Renamed 3rd party assessment to vendor assessment.
2023.02	Added security compliance and standards. Merged threat model: code review into threat modeling.
2023.07	Evolved firedrill into incident management.
2023.08	Evolved ASDM audit into internal security assessment. Renamed external pen-test to external penetration test.
2024.02	Merged awareness training and role specific training into training. Renamed status follow up to ASDM line meeting.