Axis cybersecurity framework and practices

January 2024, version 1.1

AXIS COMMUNICATIONS

Table of contents

1. Introduction 3

2. Cybersecurity framework 3

2.1 Information security policy 4

2.2 Roles and responsibilities 4

3. Axis security baseline 5

3.1 Asset management and information classification 5

3.2 Backup and recovery 5

3.3 Business continuity management (BCM) 5

3.4 Cryptography, key and certificate management 6

3.5 Identity and access management 6

3.6 Incident management 6

3.7 IT operations security 7

3.8 Network security 7

3.9 Personnel security 7

3.10 Physical security 7

3.11 Privacy protection 8

3.12 Remote working 8

3.13 Risk management 8

3.14 Secure development 8

3.15 Security awareness and training 9

3.16 System acquisition and supplier management 9

3.17 Threat intelligence 9

3.18 Vulnerability management and malware protection 9

4. Certifications and compliance 10

1. Introduction

Customers in the information, technology and security industries need assurance that the solutions being implemented in their business are safe and can be trusted. Systems and data must be accessible, but only to the intended users, and devices must be able to operate on the network without intrusion or unintended exposure. The solution must function as designed and intended, with maintained integrity and uninterrupted functionality.

At the same time, security threats are always present. New threats arise, and their nature might change at any point in time.

Axis Communications has a strong commitment to security and has processes and procedures in place to continuously address security and related risks. All employees are educated on security awareness and to exercise caution.

With this document, we want to give you an insight into Axis' cybersecurity framework and practices, which are designed to enable a systematic approach that protects the confidentiality, integrity, and availability of our assets.

2. Cybersecurity framework

Axis Information Security Management System (ISMS) is the foundation of the cybersecurity framework. The ISMS is based on the requirements in ISO 27001:2022 and facilitates continuous improvement and follow-up of Axis security posture. The ISMS is certified against ISO 27001:2022 for the scope defined on the certificate.

As part of the ISMS, Axis has implemented a cybersecurity control framework based on the controls in ISO 27002. Both the ISMS and the related security controls are audited annually by an external accredited certification body to demonstrate compliance with ISO 27001. In addition, Axis performs internal audits of the ISMS according to a yearly internal audit plan that is decided by management.

2.1 Information security policy

Axis' information security policy sets out the overall direction of Axis' security work. The information security policy is mandatory and must be adhered to by all employees, contingent workers, and consultants, as well as management and board members.

The information security policy is complemented by more detailed supporting documents, such as guidelines, routines, and the Axis security baseline (see Chapter 3 for more details). The information security policy and its underlying documents are reviewed on an annual basis and/or are updated in case of changes to Axis' overall business strategy or environment.

2.2 Roles and responsibilities

There are multiple roles throughout the organization that drive the continuous improvement of security. Axis promotes a collaborative approach to security and emphasizes that all employees have an important role to play. Examples of the roles and organizations that are dedicated to security include, but are not limited to:

> Chief Information Officer (CIO)
  - Has overall responsibility for information security and privacy at Axis
  - Is part of the corporate management team and is responsible for reporting to the board on security-related matters

> ISMS Management Team
  - Has oversight of the ISMS

> Privacy Compliance team
  - Point of contact for privacy-related matters within the company

> IT Governance
  - Is continuously developing methodology and structure around Axis ISMS

> Software Security Group (SSG)
  - SSG is the main internal contact entity for development organizations in security-related matters
  - Is responsible for the Axis Security Development Model (ASDM), a framework that defines the activities used by Axis to develop more secure software
  - ASDM is the component that represents secure development within the ISMS

> Security Operations Center (SOC)
  - 24/7/365 monitoring to detect and respond to cyberthreats

3. Axis security baseline

The Axis security baseline is the central reference for all security requirements at Axis and is a key component of Axis' information security policy.

To establish a security baseline, Axis has defined several areas with input from globally recognized security frameworks such as ISO 27001/2, NIST SP 800-53, as well as regulatory requirements such as GDPR. Below is a high-level description of the respective areas and applied practices.

3.1 Asset management and information classification

Information assets are highly valuable for Axis as an organization and shall be appropriately protected. Axis manages its assets by maintaining asset inventories and classifying assets based on their criticality. Guidance on asset management includes an asset classification scheme with defined classification levels. Asset classification is a prerequisite for efficiently protecting the confidentiality, integrity and availability of the assets.

Business and technical ownership is assigned to identified assets and documented in the asset inventory. Assigned owners are responsible for the continuous work with asset inventories and classification.

3.2 Backup and recovery

The backup and recovery procedures are designed to protect from data loss and to be able to sufficiently recover data. Backup is done at least daily, depending on the availability requirements of the data, and all backups are distributed to a secondary backup storage.

Restoration testing of backups is performed on a periodic basis using the technical solutions and tools in place.

3.3 Business continuity management (BCM)

Business continuity management (BCM) is an integral part of Axis, and various measures are implemented to ensure business continuity. Data is stored in primary and secondary data centers in different geographic locations to ensure redundancy. Assets are documented in an asset register with criticality classifications and requirements on recovery time objective (RTO) and recovery point objective (RPO).

Communication plans are in place for internal communication in case of issues with potential impact on business continuity. External communication is managed through the Axis status page on status.axis.com.

3.4 Cryptography, key and certificate management

Requirements are defined for proper and effective use and management of cryptographic keys and their associated certificates to ensure secure communication and storage of information.

Axis follows FIPS 140-3 (IEC/ISO 19790:2012) recommendations for algorithm selection where feasible with the following preferences:

> Encryption of data in motion (TLS / mTLS) - RSA 2048 and higher
> Encryption of data at rest - AES 256
> Digital signing - RSA 2048 and higher, ECDSA p256 and higher with SHA256 and higher

3.5 Identity and access management

Identity and access management (IAM) is about limiting access to physical and logical assets to only authorized users. Axis has implemented numerous security controls and practices related to IAM, both preventive and detective. Examples of security controls include but are not limited to:

> User registration/de-registration process with defined approval workflows
> Automated process for off-boarding/disabling Active Directory account of leavers
> Applying the least privilege principle
> Multi-factor authentication (MFA)
> Periodic review of user access
> Logging and monitoring of user access and activities
> Privileged account management
> Single sign-on
> Remote access management (including VPN with MFA)
> Separation of duties

3.6 Incident management

Incident management is key for business continuity and Axis has defined an incident management process to minimize the potential impact on the business and stakeholders in case of an incident. This includes detection, communication, coordination, mitigation, and resolving the incident, as well as learning from past incidents to facilitate continuous improvement.

Axis actively monitors systems and services through automated tools to detect anomalies and other indications of potential incidents. To maintain 24/7/365 incident response, Axis has established a Security Operations Center (SOC). The SOC is responsible for the continuous monitoring of security issues and are ready to act in case of identified anomalies, alarms or zero-day vulnerabilities.

Incidents are classified based on the potential business impact, escalated accordingly, and tracked in the incident management system until its resolution. An incident report is documented for all major incidents to clarify root cause and facilitate continuous improvement of the security posture.

Privacy-related incidents and potential breaches are managed according to a privacy breach management routine. The routine includes communication channels, escalation paths, assessment, and documentation. The routine is set up based on relevant privacy laws and regulations, primarily the GDPR.

External information related to incidents and status for Axis services is available on status.axis.com

3.7 IT operations security

IT operations security is about having processes, procedures, and controls to protect the operational IT environment regarding confidentiality, integrity, and availability. At Axis, this includes, for example, managing clients and servers, performing change management according to a structured and systematic process, and performing configuration management according to best practices and hardening guides.

Patch management is also an essential part of IT operations security and is managed as part of a defined lifecycle management process.

3.8 Network security

Various measures have been implemented to protect network communication to ensure access control and enable operational security.

Examples of security controls include but are not limited to:

> Role-based network access
> Requiring certificate (IEEE 802.1x) to access the corporate network
> Network segmentation
> Communication between segments must adhere to the firewall policy
> Clients connected to production networks must have endpoint protection
> Remote network access requires connecting through VPN with multi-factor authentication
> Proactive monitoring of network traffic and network equipment
> Network equipment sends logs to a central repository
> Changes to network equipment are logged

3.9 Personnel security

Personnel security is about ensuring that employees and external personnel (consultants and contractors) understand their responsibilities and are suitable for the roles for which they are considered.

In the recruitment process, guidelines are defined for security and safety. They include reference and background checks, depending on regional laws and criticality of the job role.

The process also includes security measures during and after employment, such as onboarding (granting physical and logical access), non-disclosure agreements, awareness and training and off-boarding (terminating physical and logical access when a user leaves the company).

3.10 Physical security

Procedures and routines are defined to uphold physical security, create a safe and secure environment for everyone who is working on or visiting Axis premises, and to protect Axis premises, assets, and people.

An access card and a PIN code are required in order to enter Axis premises, and anyone who is inside the premises must visibly wear an Axis badge of identification. All access to the premises is logged and logs are sent to a centralized repository. Surveillance cameras are installed throughout the premises.

Visitors must always register at Axis reception and show an approved form of identification to reception/service desk staff. Upon registration, visitors must always visibly wear a visitors' badge and are always escorted while on Axis premises.

Axis premises are divided into different security zones and access to restricted areas is limited to authorized personnel.

3.11 Privacy protection

Axis ensures that safeguards and mechanisms are in place to protect the personal data of employees, partners, and customers. Trust and Strong Brand are the core of our strategy, and we are committed to having transparent relations with end customers. We maintain their information but also always respect their right to full control of their data, in line with applicable regulations and contracts.

The following fundamental principles apply in respect to the collection and processing of personal data:

> Fairly and lawfully
> To the extent necessary
> For a legitimate purpose
> Adequate, relevant, and necessary in relation to the purpose

Further information on our privacy procedures is available at www.axis.com/privacy

3.12 Remote working

Axis has defined rules and security processes to secure devices used for remote working, such as when travelling or working from home. It covers systems and processes used to ensure work is carried out in a secure and compliant way, with distinct separation between business and non-business use.

Guidance to employees regarding remote working is provided in the security awareness training, as well as the acceptable use policy. To access internal systems and resources when working outside the office, each user is required to authenticate through a VPN connection with multi-factor authentication.

Clients and mobile devices are encrypted. Mobile devices are managed through a mobile device management (MDM) solution with possibilities for remote wiping of data if needed.

3.13 Risk management

Risk management is performed according to an annual risk management cycle, which is managed by Corporate Governance and spans over all business areas, including security. The risk management cycle includes risk assessment, risk analysis and risk follow-up. Risk analysis is presented to the Axis management team, audit committee, and the board of directors.

As part of the corporate risk management cycle, an information security risk assessment guideline is defined and applied within the ISMS. This includes continuous risk assessments and risk mitigation by system owners and risk owners throughout the organization. Identified risks are evaluated and, depending on their risk level, escalated according to a risk evaluation matrix. The CIO has the overall responsibility for the reporting of risks to management and the board of directors.

The information security risk assessment approach, methodology and implementation are externally audited on an annual basis as part of the ISO 27001 certification process.

3.14 Secure development

To enable secure development of our products and services, Axis has defined and implemented the Axis Security Development Model (ASDM). The primary objectives driving the ASDM efforts are:

> Make software security an integrated part of Axis software development activities
> Reduce security related business risks for Axis customers
> Meet increasing awareness of security considerations by customers and partners
> Create potential for cost reduction because of early detection and resolution of issues

The ASDM scope encompasses all Axis software included in Axis products and solutions. For more details on ASDM, please refer to help.axis.com/axis-security-development-model

3.15 Security awareness and training

Axis has developed a security awareness program to continuously train our employees in avoiding and mitigating security threats to the organization.

The awareness program includes security awareness training related to the information security policy and common security best practices. The awareness training is mandatory for all Axis representatives.

It also includes a safety and security training related to physical security. The training is mandatory for all personnel and contractors who access Axis premises and must be performed before the person is granted an access card to enter the premises.

Additional security training is performed, depending on organizational role and responsibilities; for example, ASDM for developers (see section 3.14 above) and role-specific awareness for system owners.

3.16 System acquisition and supplier management

Supplier vetting is carried out before entering into an agreement. This includes assessment of the potential supplier according to an assessment model covering a legal review, security assessment, and privacy assessment. Contract managers and the legal department are the main bodies responsible for vetting suppliers. They also consult various experts from within the organization, for example, security specialists.

Each supplier has a contract owner, who has the overall responsibility for following up on supplier delivery, fulfilment of contract requirements, and periodically assessing the suppliers' security.

Systems and services that are or will be procured are assessed to ensure they are in line with Axis' requirements and do not expose Axis or our partners to unacceptable risk. The system acquisition guideline addresses these requirements and must be applied when considering a new system or service.

3.17 Threat intelligence

Threat intelligence is information gathering concerning the occurrence and assessment of both digital as well as physical threats, and threat actors to help counter potential attacks and harmful events occurring in cyberspace.

Intelligence analysis and threat intelligence are performed on an ongoing basis and through multiple different sources.

Axis performs threat intelligence, both in relation to monitoring zero-day vulnerabilities and being proactive with threat intelligence by, for example, participating in security communities.

3.18 Vulnerability management and malware protection

Vulnerability management and malware protection procedures are defined to ensure that appropriate tools and methodologies are used to assess vulnerabilities and malicious code in systems or applications, and to provide remediation. Axis utilizes various scanning tools to continuously perform internal and external vulnerability scanning of our IT environment. Vulnerabilities are classified according to the Common Vulnerability Scoring System (CVSS) and prioritized based on its criticality.

Devices connected to the production network are protected and monitored by an industry-leading endpoint detection and response solution.

In relation to vulnerability management for our products, Axis applies the Axis Security Development Model (see section 3.14 above) to software for the lifecycle of a product. Axis is an authorized Common Vulnerability and Exposures (CVE) Numbering Authority (CNA) and discloses vulnerabilities transparently, according to the established framework of the CVE program. For more details on product security and vulnerability management, please refer to www.axis.com/support/cybersecurity/vulnerability-management and help.axis.com/axis-vulnerability-management-policy

4. Certifications and compliance

Axis complies with a variety of regulatory requirements, and strategically selected frameworks and standards. They are an assurance of our commitment to information security, privacy and other areas that are important to both Axis and our partners.

An up-to-date overview of related certifications and compliance can be found at www.axis.com/compliance

About Axis Communications

Axis enables a smarter and safer world by creating solutions for improving security and business performance. As a network technology company and industry leader, Axis offers solutions in video surveillance, access control, intercom, and audio systems. They are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 4,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.