WHITE PAPER

How Axis commits to the Cyber Resilience Act (CRA)

November 2026

AXIS COMMUNICATIONS

Table of Contents

1 Introduction 3
2 The lifecycle approach at Axis 3
3 CRA requirements 5
4 Essential cybersecurity requirements 5
4.1 No known exploitable vulnerabilities 5
4.2 Exploitation mitigation mechanisms and techniques 5
4.3 Secure by Default 6
4.4 Confidentiality, integrity, and availability 7
4.5 Access control and activities monitoring 7
4.6 Address new vulnerabilities with updates or patches 8
4.7 Decommissioning and removal of data 8
5 Vulnerability handling 9
5.1 CRA requirements for vulnerability handling 9
5.2 How Axis meets the CRA requirements for vulnerability handling 9
6 Information and instructions to users 9
6.1 CRA requirements for user' information and instructions 9
6.2 How Axis meets the requirements for users' information and instructions 10

1 Introduction

The Cyber Resilience Act (CRA) is a European Union (EU) regulation that focuses on improving the cybersecurity of all products that have digital network elements and are sold in the EU. The CRA aims to reduce product vulnerabilities and protect consumers and businesses. It covers devices, software, and device components.

Compliance will be indicated with the CE mark, which exists today for products sold in the EU, but will in the future reflect the added compliance for cybersecurity. Non-compliance can result in product recall, withdrawal, or fines.

CRA is product-focused and involves risk assessments and risk management for each product. It is aimed mainly at manufacturers and requires them to be responsible for their product's cybersecurity throughout the lifetime of the product. With the CRA, there is an emphasis on product lifecycle management, product vulnerability handling, Secure by Design, and Secure by Default principles.

CRA complements *EU's NIS2 Directive* (Network and Information Security Directive 2), a unified legal framework designed to strengthen the cybersecurity and resilience of critical sectors. NIS2 is focused on the organization and the responsibility that essential and important entities in the EU need to undertake to ensure resilience. Such organizations are required to assess and manage cybersecurity risks, look at how their suppliers are handling the security of their products and services, and to manage any cybersecurity incidents. CRA is instead a regulation that applies directly to all manufacturers on the EU market. To read more about how Axis products help customers meet the requirements for NIS2, see *NIS2 White paper*.

This white paper shows how Axis meets the requirements of the CRA, and in many cases goes beyond what is generally required in the industry.

For more information about the regulation, see *Cyber Resilience Act*.

2 The lifecycle approach at Axis

The lifecycle approach to managing product security is about addressing the security needs of a product throughout its lifecycle, not simply at one point in a product's lifetime. At each stage of a product lifecycle, there are security risks that should be addressed and mitigated. Axis has been taking the *lifecycle approach* for many years and supports the security needs of its products long before and after they've been sold and installed.

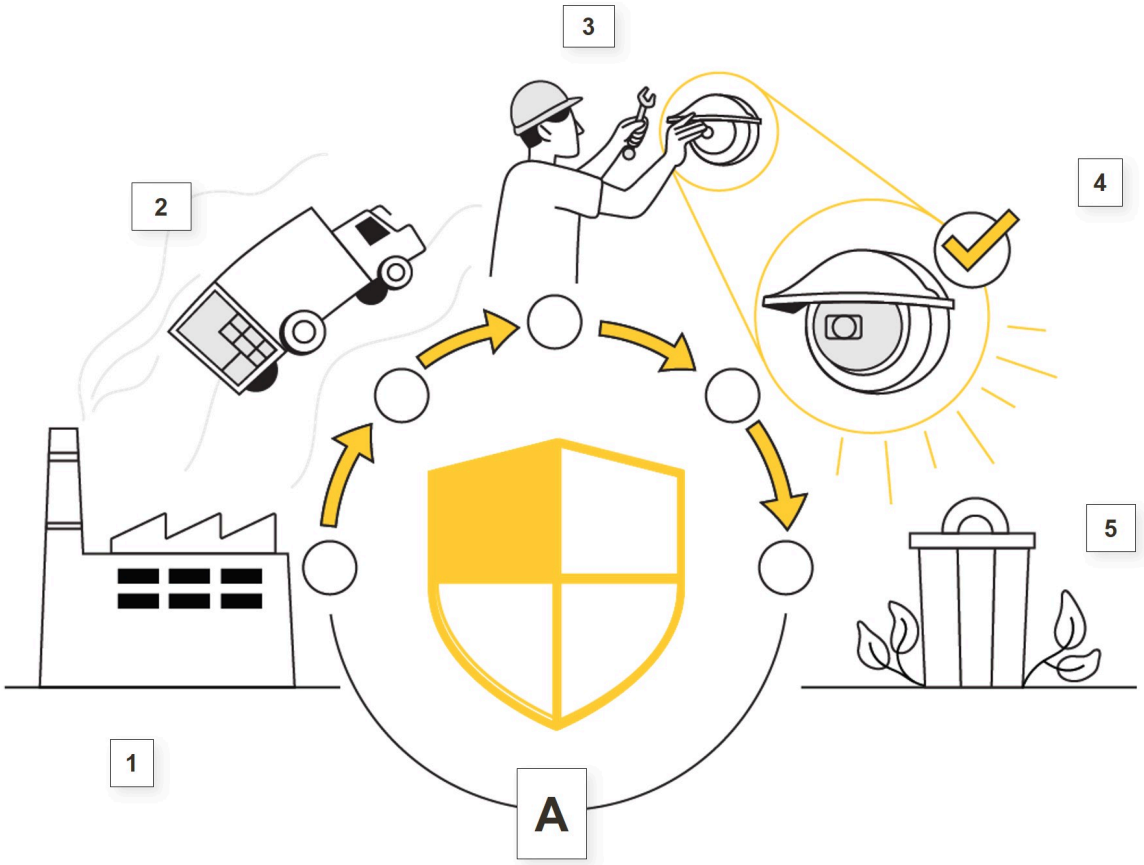

Figure 2.1 *Security throughout our products' lifecycle, enabled by (A) a firm security foundation.*

1 *Production*
2 *Distribution*
3 *Implementation*
4 *In service*
5 *Decommissioning*

- **Security foundation:** The security foundation of Axis offerings rests on four key elements that help mitigate the risk of vulnerabilities in Axis products and support all aspects of their cybersecurity.
  - *Axis Security Development Model* (ASDM) for software, including device software, outlines the activities that all software development teams at Axis need to undertake to reduce software vulnerabilities.
  - *AXIS OS*, the device software or operating system that runs and helps secure Axis devices.
  - *Axis Edge Vault*, the hardware-based cybersecurity platform that safeguards the integrity of Axis devices and enables the execution of secure operations based on cryptographic keys.
  - Axis' commitment to the principles of transparency, especially as it relates to *vulnerability management*.
- **Production and distribution phases:** In these phases, Axis takes steps to secure the supply chain and production, for instance:
  - Critical components are procured directly from certified strategic suppliers.
  - Axis works closely with manufacturing partners where production processes are monitored and data is shared 24/7 with Axis.
  - There are mechanisms in place that mitigate the risk of malicious modifications during shipment.

- **Implementation phase:** When products are being installed in the implementation phase, Axis makes sure that protective measures are in place by default to protect sensitive data and communications, and that there are measures that enable customers to control access and monitor activities.
- **In-service phase:** This is the phase where Axis products are in operation and we provide software updates to fix any newly discovered vulnerabilities and disclose them in a transparent but responsible manner to help customers maintain the security of Axis devices.
- **Decommissioning phase:** We provide information about end of software support dates and how to remove all data and configurations. This helps users to prepare for proper decommissioning of products.

3 CRA requirements

The CRA requirements can be broken down into three main areas:

- Essential cybersecurity requirements
- Vulnerability handling
- Information and instructions to users

4 Essential cybersecurity requirements

The security requirements reflect the product lifecycle approach to managing security, and the principles of Secure by Design and Secure by Default. For example, the products must:

- Not contain any known exploitable vulnerabilities.
- Have Secure by Default configurations.
- Have regular updates or patches to address newly discovered vulnerabilities.
- Ensure confidentiality and integrity of data and protect the availability of essential and basic functions.

4.1 No known exploitable vulnerabilities

This requirement is best addressed by the Secure by Design principle. The specifics of what is covered under this principle can vary depending on a country's or organization's interpretation of it. But generally, the approach is about integrating cybersecurity best practices from the earliest stages of product development, rather than something to be addressed later.

Axis has been addressing the need to mitigate the risk of vulnerabilities in software for years through Axis Security Development Model (ASDM). The model outlines the activities that all software development teams at Axis need to undertake to reduce software vulnerabilities throughout a product's lifecycle, from the start when determining product requirements, after product release, and to the end of a product's lifetime.

The development model for software prescribes activities like risk and vendor assessments, threat modeling, static code analysis, and software composition analysis (necessary for producing a Software Bill of Materials), as well as threat model and external penetration testing, among others. After a product is sold, activities like vulnerability and incident management are involved. Axis goes further than many companies, by supporting bug bounty programs that cover, for instance, AXIS OS products.

CISA, the U.S. Cybersecurity & Infrastructure Security Agency, encourages manufacturers to commit to the Secure by Design principle. Axis signed the *CISA pledge* in 2025 to demonstrate this commitment.

4.2 Exploitation mitigation mechanisms and techniques

Axis addresses this requirement primarily through the hardware-based cybersecurity platform, Axis Edge Vault, together with the device's operating system, AXIS OS.

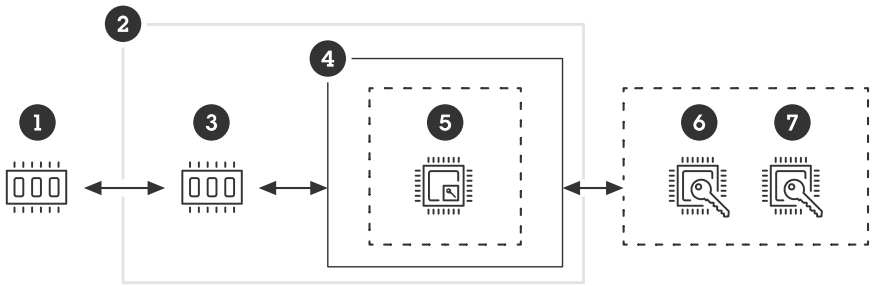

Figure 4.1 *The diagram illustrates the various elements of Axis Edge Vault. Cryptographic computing modules (5, 6, and 7 in the diagram) provide secure storage of cryptographic keys that Axis or customers provide to devices for use in secure operations. Axis cryptographic keys, for instance, are used for the Axis device ID, which is an ID unique to the particular unit and ensures the device is genuinely from Axis. The keys are also used in secure operations like device authentication and data encryption on HTTPS or IEEE 802.1X networks.*

1 *Flash memory (for signed OS, read-write file system)*
2 *System-on-chip (SoC)*
3 *Boot ROM (for secure boot)*
4 *CPU*
5 *TEE (for secure keystore)*
6 *Secure element (for secure keystore)*
7 *TPM (for secure keystore)*

Boot ROM and flash memory support signed OS to ensure that the device only boots with genuine device software. This prevents unauthorized device software from being deployed on Axis products. The combination of secure boot and signed OS, together with making a factory default, safeguards against the threat of malicious modifications during shipment. This is part of ensuring device integrity and enabling supply chain protection.

Another measure that supports CRA's exploitation mitigation mechanism requirement is brute force delay protection. This mechanism in AXIS OS products mitigates the risk of password guessing. And to limit attack surfaces, less secure protocols in AXIS OS products are disabled by default.

4.3 Secure by Default

The CRA requires Secure by Default configurations to enable protection out of the box and minimize risk of misconfigurations and exposure to attacks. Products should be safe to use from the start without the need for immediate hardening or advanced setup. This requirement is mainly aimed at consumer products where end users might lack cybersecurity knowledge and skills.

Axis aims to reduce the need for hardening guidelines by increasing the *Secure by Default configurations*. The following are the default settings for devices running the latest AXIS OS today:

1 Secure onboarding and encrypted communications (through support for IEEE 802.1X/802.1AR/802.1AE) are enabled by default.

2 Brute-force delay protection is enabled by default.

3 There is no default password. A device can't operate until an admin password is set and strong password rules apply to new accounts.

4 Only HTTPS is enabled by default for communications between a client and device.

5 Devices can only run ACAP applications that are signed, to ensure only authentic applications are installed on an Axis device.

6 UPnP Discovery Protocol is removed.

7 Signed video is enabled by default. Signed video is a feature that allows you to verify if a video recording from an Axis camera is authentic and hasn't been tampered with.

Communications are encrypted by default between Axis video management software and Axis devices, and also in device to cloud connectivity.

4.4 Confidentiality, integrity, and availability

Axis products support this CRA requirement by supporting encryption for device and network security. Device security is primarily provided by Axis Edge Vault platform. It enables secure storage of cryptographic keys used for encryption, and supports Axis signed video.

Also, Axis Edge Vault enables a device's file system to be encrypted when not in use. This protects customer-specific configuration and information stored in the file system from being extracted or tampered with while the device is, for instance, in transit from a system integrator to the end customer, or if the device is stolen.

Additionally, Axis devices support the possibility to encrypt data stored on a local SD card, as well as export a recording that's already password-based encrypted on an SD card, network share, or an AXIS OS-based recorder to securely share sensitive video data with third parties without the need for manual, external encryption tools. It prevents unauthorized individuals without the password from being able to play exported video material.

Host-based firewall support on Axis devices allows the devices to control the kind of network traffic, particularly incoming, that is allowed to protect against unauthorized access and attacks.

When it comes to network security, Axis products support HTTPS for encrypted communications between a device and client, whether locally or remotely. Axis devices also support secure streaming using SRTP (Secure Real-time Transport Protocol) and RTSP over TLS (RTSPS). Depending on the deployment, these protocols can be used individually or together. RTSPS secures control and signaling. SRTP secures media (video/audio/metadata) by encrypting and authenticating RTP traffic while keeping latency low, which is important for real-time media streaming. Together, they protect the streaming session and the data in transit, ensuring that only authorized clients with support for these protocols can access the stream.

Going further than what most companies offer, Axis products have support for IEEE 802.1X, 802.1AR and 802.1AE MACsec standards that make zero-trust networking easier. You can leverage the IEEE 802.1AR-compliant Axis device IDs to ensure only authorized devices connect to the network, and with MACsec, you automatically have an extra layer of encryption for a variety of data, on top of HTTPS and SRTP.

The downloads of software security updates available on axis.com come with accompanying integrity checksum to enable users to check the integrity of the file.

4.5 Access control and activities monitoring

When it comes to the CRA requirement for controlling access and monitoring activities, Axis supports a number of mechanisms.

Axis hardware and software products support role-based device management access rights like administrator, operator, and viewer access. Going further than what most companies in the industry offer, Axis products also support centralized authentication and authorization by enabling Axis devices, with support for *OAuth 2.0 OpenID Connect* authentication schemes, to connect to IT-standardized Active Directory Federation Service (ADFS) integrations and other Identity provider solutions for single sign-on capabilities and multi-factor authentication.

AXIS OS products and Axis video management software also support audit logs to monitor network activities, configuration changes, login attempts, compliance with security policies, and identification of possible unauthorized access.

Axis devices support system log (syslog), which is an IT industry standard format for message logging in IT devices, and remote syslog. AXIS OS products preserve their configuration and forensic audit logs during and after an incident like a denial of service-attack, allowing you to forensically analyze the product after an incident. For example, see *AXIS OS - Forensics guide*.

4.6 Address new vulnerabilities with updates or patches

CRA requires manufacturers to provide security updates or patches to address newly discovered vulnerabilities. The *AXIS OS platform* helps us to quickly and efficiently release security patches across a great number of products. AXIS OS security updates are available through two main tracks: active track and long-term support (LTS) track.

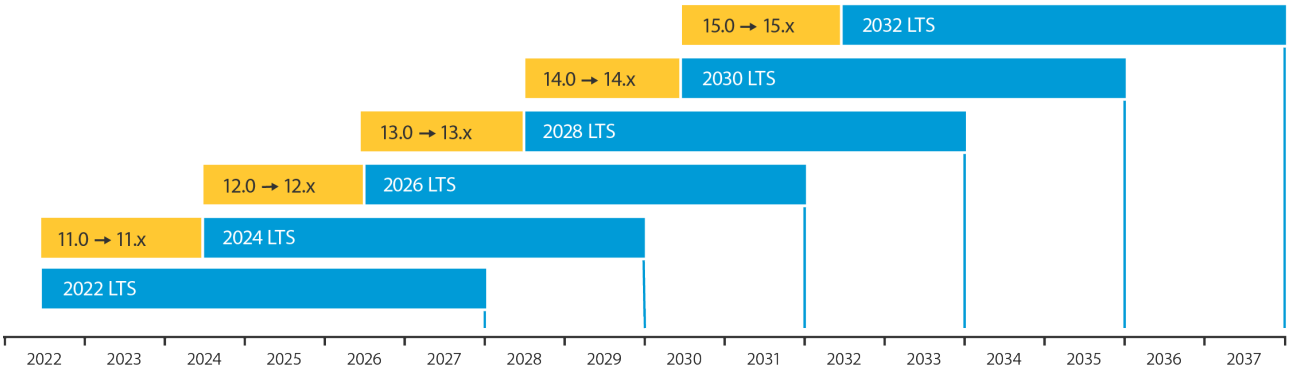

Figure 4.2 *In the image above, yellow represents the active track and blue, the LTS track.*

When Axis releases a new AXIS OS-based device, only the active track is available for that device. An AXIS OS release on the active track includes new or enhanced OS features, as well as security updates and bug fixes. AXIS OS releases a new version every 2–3 months and only the latest version is supported.

Within two years of a new product release, an LTS track becomes available as an alternative to the active track. On the LTS track, AXIS OS updates involve only patches and bug fixes since the focus is on consistency and keeping a well-integrated third-party system. When a device is discontinued, it's moved to the LTS track where it's supported with patches and bug fixes for five years.

A new active track and LTS track for a device are introduced every two years. During the lifetime of a device, that device can have only one active track but several LTS tracks. If there are no system compatibility issues, Axis advises customers to continue on the active track in order to be able to benefit from new cybersecurity features.

4.7 Decommissioning and removal of data

The CRA requires manufacturers to provide users with a secure and easy way to permanently remove all data and settings from a product. This is an essential security capability when decommissioning a product.

Users should plan to decommission a product before it reaches its end of software support date. After this date, the manufacturer no longer addresses newly discovered security vulnerabilities or provides security updates for the product. Continuing to operate a product beyond its end of software support date may expose the system to security risks if new exploitable vulnerabilities are discovered.

For many Axis products, the end of software support date is published on the product support web page. This information helps users plan for the timely replacement and decommissioning of products. Device management software can also help by tracking warranty status, product discontinuation and end of software support dates across all devices in a system.

When decommissioning an Axis device, perform a factory reset to restore the device to its default settings and permanently erase all user configurations and data.

5 Vulnerability handling

5.1 CRA requirements for vulnerability handling

Manufacturers shall document vulnerabilities and components contained in products, including a software bill of materials (SBOM). Manufacturers must also regularly test and review the security of their products, have policies in place for handling vulnerabilities and their disclosures, and address vulnerabilities with security updates or patches that are communicated and provided in a timely manner.

5.2 How Axis meets the CRA requirements for vulnerability handling

- **Documenting vulnerabilities:** Axis transparently documents its vulnerabilities on *axis.com* and *cve.org*, the CVE (Common Vulnerabilities and Exposures) website. Axis is a CVE Numbering Authority (CNA) and is, therefore, able to issue CVE IDs.
- **Documenting components, including a software bill of materials:** At Axis, SBOMs are derived from the software composition analysis activity conducted as part of the Axis Security Development Model. While CRA doesn't require external publication of an SBOM for a product, Axis already makes SBOMs externally accessible on product web pages for AXIS OS-based products, network video recorders, and Axis video and device management software. SBOMs essentially list the components that make up the software, and SBOMs can be used to perform vulnerability analysis to evaluate the risk of a product.
- **Testing and reviewing product security:** The *Axis Security Development Model* includes threat model testing and external penetration testing prior to a software release. After a software release, we continually address vulnerabilities that are newly discovered, whether from internal or external work, or from Axis bug bounty programs, which reward ethical hackers and security researchers if they find vulnerabilities.
- **Addressing software vulnerabilities:** Axis provides security updates for both device software and software applications. Security updates for AXIS OS-based devices will always be included in new AXIS OS versions, whether they are versions on the active or long-term support tracks. Axis provides a host of information on *axis.com* about how software vulnerabilities are handled. Depending on the vulnerability level, the policy outlines the timeframe for when customers can expect Axis to resolve an identified vulnerability, and when and how a vulnerability is communicated. Axis coordinates vulnerability disclosures with external security researchers who find a vulnerability. The security advisories outline the vulnerability in a responsible way and provides instructions on what actions users need to take.

  Going beyond what's required, Axis mitigates critical vulnerabilities at the network layer by collaborating with Palo Alto Networks. Joint customers benefit from Palo Alto Networks' virtual patches, which provide air cover and give customers time to thoroughly test and deploy official Axis software updates without being exposed to security risks.
- **Disseminating information:** Axis makes public disclosures of its software vulnerabilities through cve.org, axis.com, and directly to subscriber's email through the Axis security notification service.
- **Distributing security updates:** Security updates for software are available on axis.com and notified through a number of channels. Notifications of updates are available on video management software applications like *AXIS Camera Station Pro*, *AXIS Camera Station Edge*, *Milestone* and *Genetec* VMS, and through the use of *Axis device management software* and *Cisco Meraki's cloud-based dashboard* for device management. These interfaces allow you to manage and update device software directly. Axis device management software can support OS updates on hundreds of AXIS OS-based products simultaneously.

6 Information and instructions to users

6.1 CRA requirements for user' information and instructions

CRA requires products to be accompanied by specific information and instructions for the user. This includes, for example, manufacturer's contact information, vulnerability management information, product details such as a unique ID, purpose of the product, outlined risks, and EU declaration of conformity. CRA also requires manufacturers to detail the type of support provided, the end date for the support period, and hardening guides.

6.2 How Axis meets the requirements for users' information and instructions

- **Contact information, vulnerability reporting and policy:** Axis website and product documentation provide this information.
- **Product details:** Axis hardware products come with a serial number printed on the product label. Axis devices with Edge Vault also have a unique Axis device ID, which conforms with the IEEE 802.1AR standard that can be verified using the *Axis device ID certificate chain*. Information about the purpose of Axis products is available on the products' web page or datasheet, risks are outlined in product hardening guides, and EU Declaration of Conformity documents are available on the products' support web page.
- **Support period and hardening guides.** When it comes to end of software support period for AXIS OS-based products, you can find this information on the product's web page. Axis hardening and integration guides, as well as web pages like the *AXIS OS Knowledge Base*, provide information and recommendations on how to configure a product or set up a system for optimal cybersecurity. Axis also goes further by providing other types of guides like *AXIS OS Vulnerability Scanner Guide* and *AXIS OS Forensics Guide*. The vulnerability scanner guide offers recommendations on how to solve certain remarks from vulnerability scanners. In the event of a cyber attack on a network where Axis devices are installed, the AXIS OS Forensics Guide provides a baseline of forensic checklists and inspection techniques that will help customers understand if Axis devices were compromised.

For more information about Axis cybersecurity, see *Axis cybersecurity portal*.

T10245426/EN/M1.7/2611

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 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.

© 2026 — Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC and VAPIX are registered trademarks of Axis AB in various jurisdictions. All other trademarks are the property of their respective owners. We reserve the right to introduce modifications without notice.