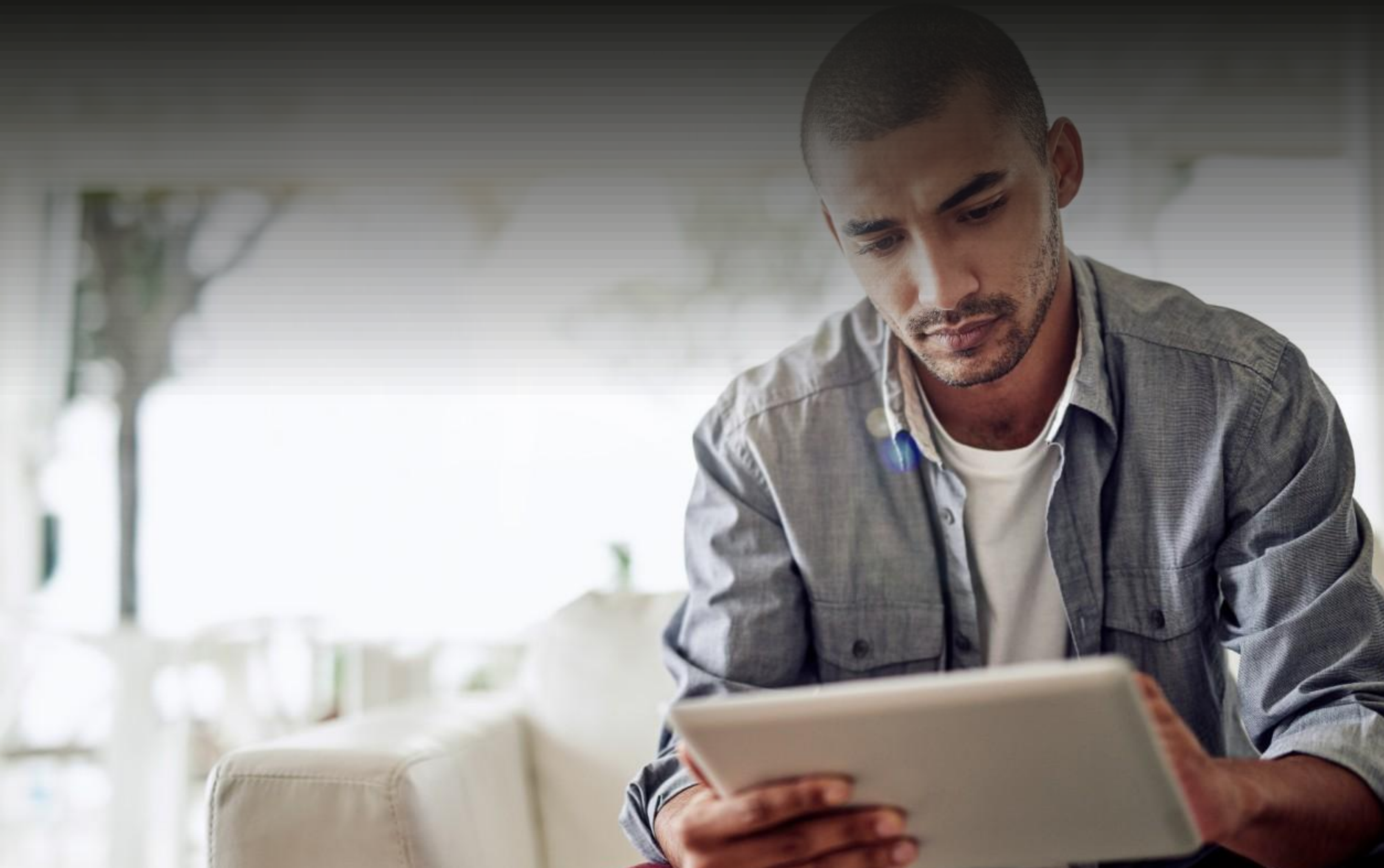
From Compliance to Cyber Resilience: Navigating NIS 2, CRA and the Future of EU Cybersecurity Regulation

THOUGHT LEADERSHIP PAPER

SEPTEMBER 2025



Contents

The Shift in Cybersecurity Paradigm: From Isolated Protocols to Integrated Strategies

Historically, businesses relied on separate security protocols and focused on protecting specific organizational assets, such as networks, data, or endpoints, and companies' CIOs and CISOs oversaw all these activities. However, these standalone methods and security fixes don't cut it anymore. As attackers get smarter and systems become more connected, organizations need complete, integrated security strategies that protect their entire network.

The increasing popularity of "living off the land" attacks, which use legitimate organizational network tools, requires organizations to develop sophisticated detection and response systems. Such attacks are often state-sponsored and use cyber power to achieve political goals, which blurs the lines between corporate and national security. The ransomware attacks on suppliers show how cyber threats affect multiple critical sectors, such as healthcare, finance and manufacturing.

Between January 2024 and April 2025, Europe experienced a substantial number of cyber incidents, with technology being the most targeted sector, followed by public and financial sectors.

Figure 1: Targeted Sectors per number of incidents for the time period Jan 2024 – April 2025

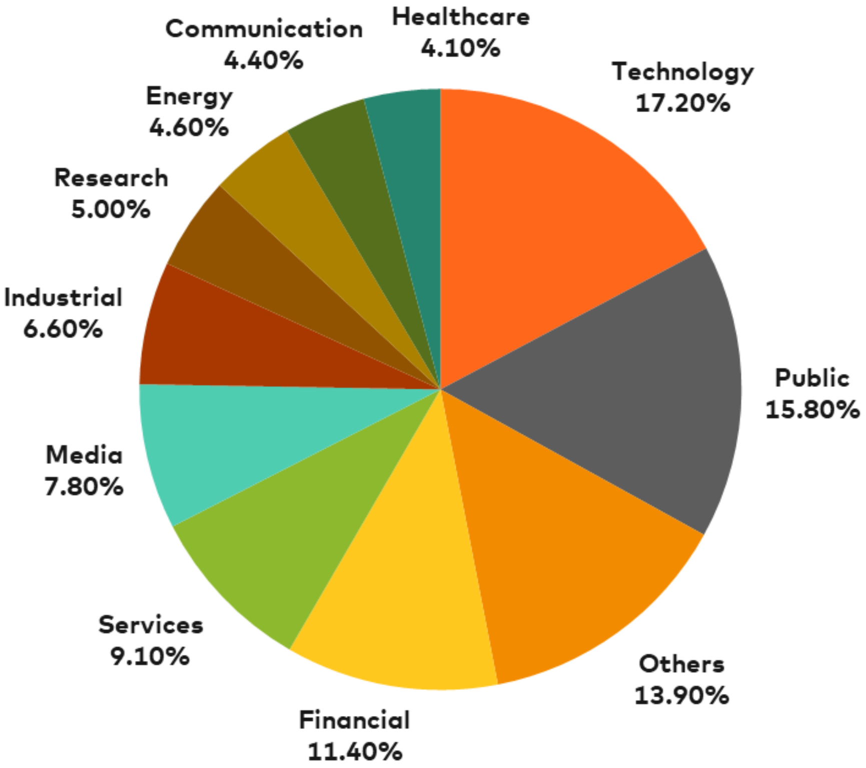
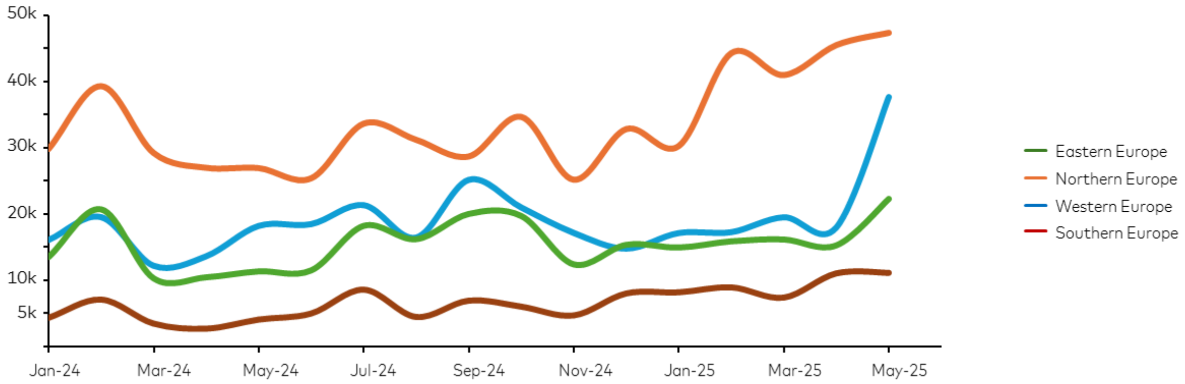


Figure 1A: Targeted regions in Europe per number of incidents



The European Union (EU) has recognized the systemic nature of these events and put in place an ambitious set of regulatory frameworks to address them. The NIS 2 Directive and Cyber Resilience Act (CRA) are among the main regulatory frameworks that aim to enhance digital resilience across EU member states and ensure a more coordinated response to emerging security threats and incidents. With these regulations, the EU tends to make cybersecurity a vital topic on the EU members' agendas, which governments and organizations should treat as a strategic priority through collaborative efforts.

NIS 2 and CRA Overview

NIS 2 Overview

The NIS 2 Directive (2022) aims at improving the cybersecurity of critical infrastructure and essential services, updating and replacing the original NIS Directive (2016). The new directive has an increased number of regulated sectors (18 instead of 7), adds stricter measures for risk management, introduces incident reporting requirements and makes senior management more accountable. The main goal of these changes is to create a common set of cybersecurity measures across the EU to ensure a unified approach in protecting countries' critical infrastructure.

On the other hand, CRA is aimed at manufacturers of products with digital components. The CRA is different from the NIS 2 Directive in that it focuses on the cybersecurity of digital products throughout the product lifecycle, as opposed to the operational cybersecurity of critical entities. The CRA seeks to enhance supply chain security and protect end-users by requiring producers to implement strong cybersecurity measures.

Here we give an extensive evaluation of the NIS 2 and CRA regulations by various criteria and analyze their similarities, differences and combined impact on EU cybersecurity infrastructure.

Regulation Purpose

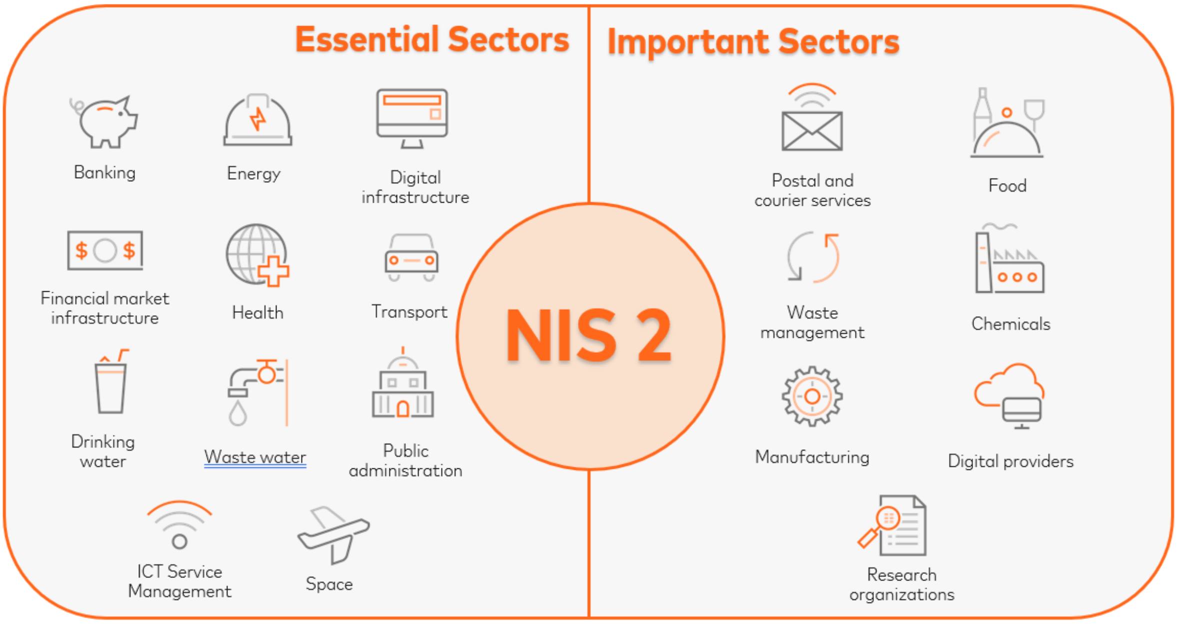
NIS 2 works to establish a high uniform cybersecurity standard across the EU for essential and important sectors, which enhances the market and social systems' resistance against cyber disruptions. NIS 2 is a fundamental element of the EU Digital Decade Programme and aims to enhance and standardize cyber capabilities and incident response systems of vital services across Member States.

Scope and Object of Regulation

The regulation applies to operators within specified essential and important sectors, such as energy, transport, healthcare, banking, etc., mentioned in Annex I and Annex II. All medium and large organizations within those sectors must comply with regulation. While smaller businesses are usually excluded, critical companies need evaluation for inclusion (e.g. the sole provider of a service in a Member State or impacting public safety). Major DNS and trust service providers together with telecom networks are also included regardless of their size. The framework also includes government agencies as participants except for defense, national security and law enforcement agencies. Every member state needs to identify the entities that fall under its regulatory oversight and notify them. The

NIS 2 will regulate approximately 160.000 EU businesses according to Infosecurity Europe.

Figure 2: NIS 2 Perimeter Explained



Level of Regulation

The regulation primarily uses principle-based standards to establish a high common level of cybersecurity through risk-based measures. The regulation sets general objectives and requirements instead of specific regulations and depends on Member State implementation. NIS 2 framework represents an advanced version of NIS and incorporates multiple years of learned experiences.

Timelines of Regulation

The deadline for EU member states to adopt it into national standards is October 17, 2024. The new regulation started to be enforced on October 18, 2024.

Affected Roles

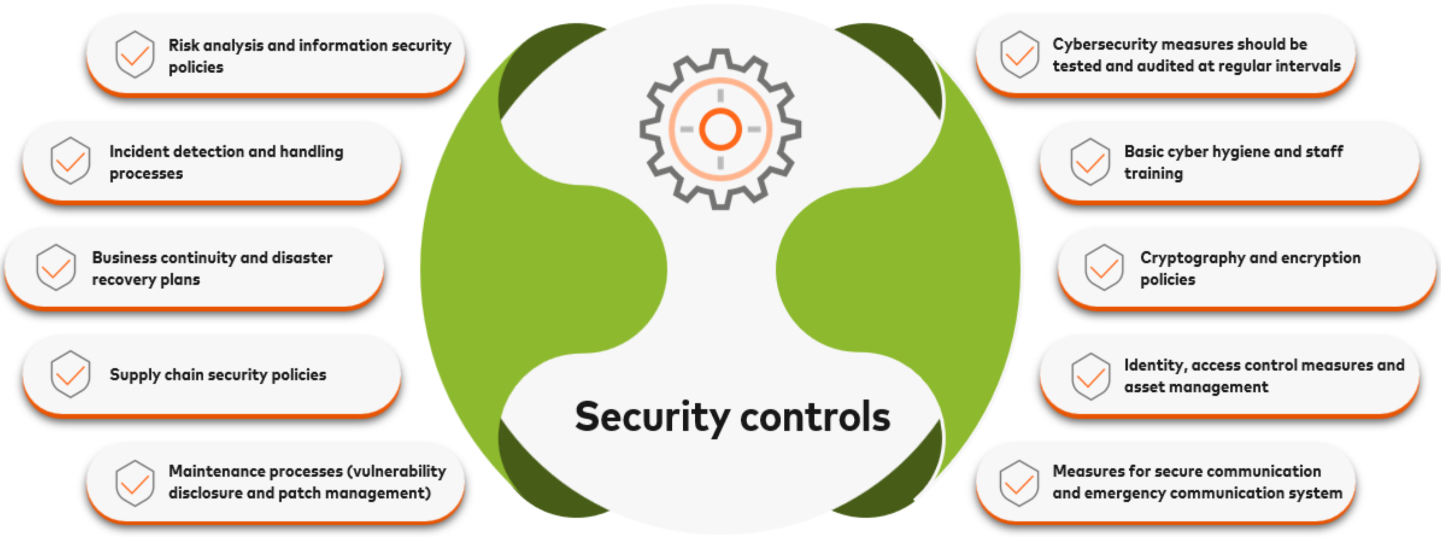
The regulation leads to immediate action through the CISO, cybersecurity team and risk & compliance officers within an organization. Organizations need to designate someone who will both implement security measures (typically the CISO) and report incidents to the organization. NIS 2 mandates executive management involvement alongside the board. It requires management bodies to approve cybersecurity measures and impose liability for non-compliance. NIS 2 establishes cybersecurity as a matter which requires board-level attention.

The operational teams who handle IT and OT security functions work to establish technical controls and develop incident response plans. Risk management professionals take charge of conducting necessary risk assessments and audits.

Security Requirements

NIS 2 broad organizational security controls include the following:

Figure 3: NIS 2 Security controls

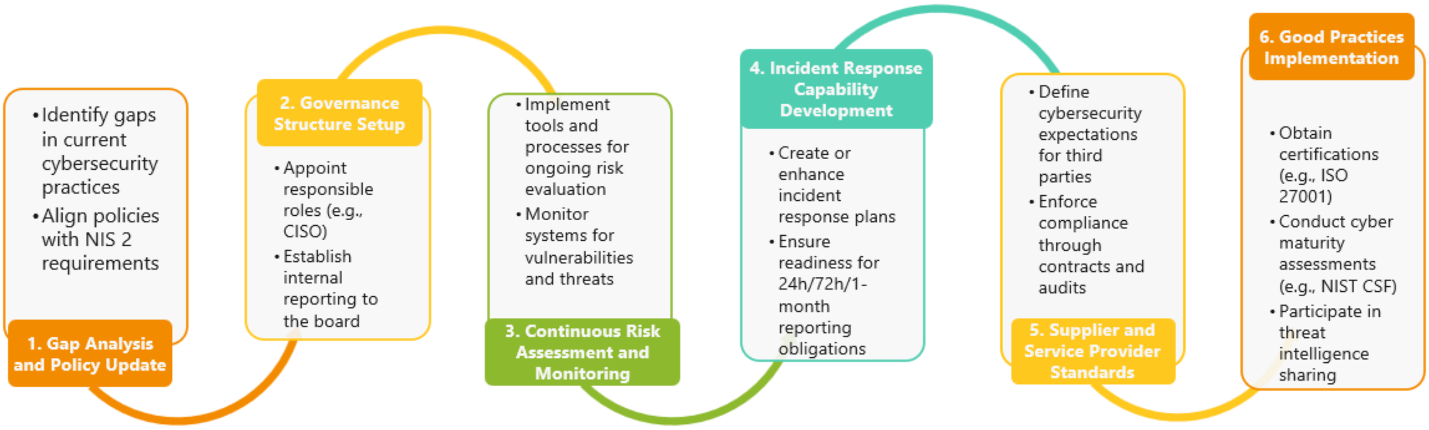

Risk analysis and information security policies
Incident detection and handling processes
Business continuity and disaster recovery plans
Supply chain security policies
Maintenance processes (vulnerability disclosure and patch management)
Security controls
Cybersecurity measures should be tested and audited at regular intervals
Basic cyber hygiene and staff training
Cryptography and encryption policies
Identity, access control measures and asset management
Measures for secure communication and emergency communication system

Organizations are allowed to select their own security frameworks or certifications as a way of meeting the requirements. It's a common practice to use standards, such as ISO/IEC 27001 or the NIST cybersecurity framework. In summary, NIS 2 requires an ISMS approach that encompasses all the aspects of information security.

Main Compliance Requirements & Actions

Companies subject to NIS 2 must undertake several steps:

Figure 4: NIS 2 compliance actions



1. Gap Analysis and Policy Update

- Identify gaps in current cybersecurity practices
- Align policies with NIS 2 requirements

2. Governance Structure Setup

- Appoint responsible roles (e.g., CISO)
- Establish internal reporting to the board

3. Continuous Risk Assessment and Monitoring

- Implement tools and processes for ongoing risk evaluation
- Monitor systems for vulnerabilities and threats

4. Incident Response Capability Development

- Create or enhance incident response plans
- Ensure readiness for 24h/72h/1-month reporting obligations

5. Supplier and Service Provider Standards

- Define cybersecurity expectations for third parties
- Enforce compliance through contracts and audits

6. Good Practices Implementation

- Obtain certifications (e.g., ISO 27001)
- Conduct cyber maturity assessments (e.g., NIST CSF)
- Participate in threat intelligence sharing

Good practices of compliance include obtaining certification, for instance ISO 27001 (to show a level of control), conducting regular cyber maturity assessments (e.g., NIST CSF), and participating in cyber threat information sharing.

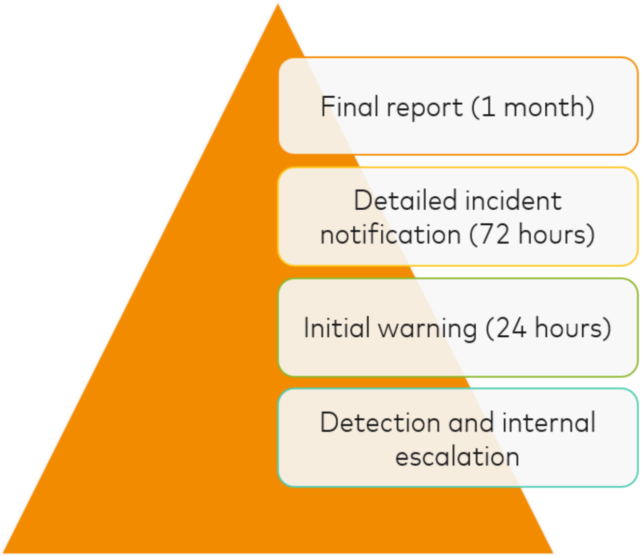
Reporting Obligations

Under NIS 2, there's a very detailed incident reporting system for significant incidents. An entity must notify the national CSIRT or competent authority of an incident whenever it affects the entity's services significantly (criteria include major service disruption or financial loss, or a large number of people affected).

The notification must be done "without undue delay" in stages: an initial warning within 24 hours of detecting an incident, a more detailed incident notification within 72 hours, and a financial incident report with root cause analysis and mitigation details within one month after resolution. Entities also must inform service recipients without undue delay if an incident is likely to adversely affect them (e.g. a cloud provider must inform its customer base of a major outage/security event). Additionally, entities are expected to notify their recipients of the existence of a notable cyber threat that has not yet turned into an incident in order to advise them on how to prevent any harm.

The Directive aims to simplify the process of reporting; notably, if several laws are applicable (for instance, if the incident is both a NIS 2 and a GDPR personal data breach) there is a vision of a single point mechanism for notifications. The templates and procedures for NIS 2 incident reporting will be determined by the authorities of ENISA, however, the very tight timeframes (24h/72h) mean that CISOs need to have a plan in place that includes notifying the regulators. Non-compliance may result in fines. In practice, organizations should have internal escalation procedures in place to identify NIS 2 incidents quickly and have a designated team to handle communication with authorities.

Figure 5: Alert Escalation Pyramid


Final report (1 month)
Detailed incident notification (72 hours)
Initial warning (24 hours)
Detection and internal escalation

Enforcement Mechanism

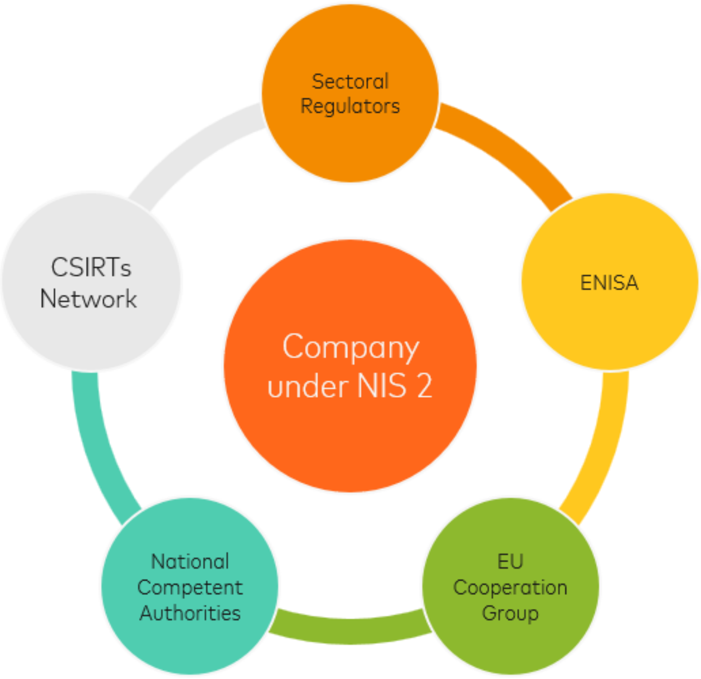
NIS 2 is enforced by national competent authorities (NCAs) designated by each member state. Often this will be a national cybersecurity agency or sectoral regulators. These authorities have powers to supervise and audit entities - they can request documentation of NIS 2 compliance, perform or commission security audits and inspections, and require information about an entity's security measures. If they find deficiencies, they can issue binding instructions or orders to remedy gaps within a set timeframe. In cases of severe non-compliance they can impose administrative fines or other measures like suspending a service.

NIS 2 also fosters cooperation among the authorities. There is an EU Cooperation Group (strategic coordination and best practice exchange among the Member States) and a CSIRTs network (for operational sharing of incident info). ENISA (the European Union Cybersecurity Agency) plays a support role, developing guidelines, facilitating exercises and receiving aggregated incident data every quarter from national SPOCs.

There is also a mechanism for peer reviews. Member states authorities can voluntarily evaluate each other's capabilities. Enforcement is therefore multi-level. Local authorities handle day-to-day compliance and incident oversight, while at the EU level, there is policy alignment. Some sectors (e.g., banking, energy) might use their sector regulations in coordination with the NCA. Companies can expect that their NIS 2 regulator may periodically inquire about their risk assessments, security policies and may follow up after major incidents.

Audits could be triggered especially if an incident revealed weak measures. NIS 2 Directive also ensures management accountability. Theoretically executives could face individual liability under national law for gross negligence in cybersecurity (though specifics depend on national transposition). Finally, the Cooperation Group and ENISA will develop guidance documents to harmonize how enforcement is done so that, for example, what Germany considers appropriate measures is similar to what France or others do.

Figure 6: NIS 2 Enforcement Ecosystem



Penalty Severity

NIS 2 requires member states to implement "effective, proportionate and dissuasive" penalties for infringements. The directive sets minimum maximum fines that must be available:

- ✓ For essentials entities, up to €10 million or 2% of worldwide turnover, whichever is higher, for serious violations (for example, failing to implement risk measures or report incidents).
- ✓ For important entities, up to €7 million or 1.4% of turnover, whichever is higher.

These caps are a bit below GDPR, which is 4% or €20 million for top tier, but still very substantial, so it may be potential business ending for smaller companies.

NIS 2 leaves it to national law to decide exact fine levels and lesser offenses. Factors like the nature of infringement, intent or negligence, previous violations and mitigating actions will be considered by regulators when setting fines. The directive also allows other penalties: for example, orders to cease certain activities, or for public sector entities, possibly exclusion from funding. While NIS 2 doesn't directly impose personal liability, member states can choose to impose penalties on individual managers in line with their legal systems. In essence, penalty regime is "GDPR- like", as it introduces the threat of multi-million fines to motivate compliance, but the exact enforcement posture may vary by country. You can expect that regulators will reserve maximum fines for some extreme use cases (for example, an essential service provider utterly fails to secure systems or blatantly ignores incident reporting). Nonetheless, CISOs should brief their boards that non-compliance can lead to penalties comparable to data protection fines and thereby they must invest in cybersecurity.

CRA Overview

Regulation Purpose

CRA aims at ensuring the cybersecurity of products through the manufacturers' implementation of sound security measures and obtaining certifications. The internal market will achieve secure-by-design products through the CRA's objective to "ensure more secure hardware and software products", which will reduce widespread vulnerabilities. Manufacturers must prioritize cybersecurity throughout the complete product lifecycle starting from the design and development phases. CRA aligns with the EU's goal to protect both consumers and businesses from insecure devices.

Scope and Object of Regulation

CRA implements a broad horizontal regulation, which applies to producers, distributors and importers of physical hardware with embedded digital elements, which can be connected to a device or network. The CRA scope also encompasses software component of such products as well as solutions provided in a SaaS fashion if they qualify as remote data processing solutions. The products that are in CRA scope will fall into different categories depending on their risk level and criticality. Examples of products subject to CRA requirements include firewall appliances, IoT thermostats, microcontrollers, CPUs, etc. (full list of products is defined in Annex III and IV). CRA aims to ensure that these products meet stringent cybersecurity requirements before entering the EU market.

Figure 7: CRA product categories explained

Default	Important "Class I"	Important "Class II"	Critical
• Smart speakers • Hard drives • Domestic robots • Wearables • Gaming consoles • Streaming devices • Smart TV	• Identity management and privileged access management systems • Network management systems • SIEMs • VPNs • Routers, modems	• Hypervisors and container runtime systems • Firewalls, intrusion detection and/or prevention systems • Tamper-resistant microprocessors and microcontrollers	• Smartcards or similar devices • Smart meter gateways and other devices for advanced security purposes (e.g. secure cryptoprocessing) • Hardware devices with security boxes

Open-source developers who operate without commercial motives receive an exception to the manufacturer classification. Some products are also exempt from CRA, because they have already fallen under sector-based regulations. For example, medical devices and automotive vehicles require cybersecurity standards in their own EU regulations, so they may receive an exemption from CRA to prevent dual oversight. The Act extends its product-focused coverage to all sectors including both industrial control systems, consumer IoT devices and smart toys. The CRA covers a much wider range of products because of its sector-agnostic approach.

Level of Regulation

CRA is more prescriptive and detailed and explicitly sets cybersecurity requirements for product design, development and maintenance processes. It reads like a product safety law and enumerates specific technical requirements and conformity procedures.

Timelines of Regulation

The European Parliament adopted CRA in March 2024 and the Council took up its adoption during the remainder of 2024. CRA will not apply immediately, it has a grace period. Most provision with start applying mid-2026 for reporting obligations and mid-2027 for product compliance. This gives manufacturers a transition period to adjust product designs and compliance processes.

Affected Roles

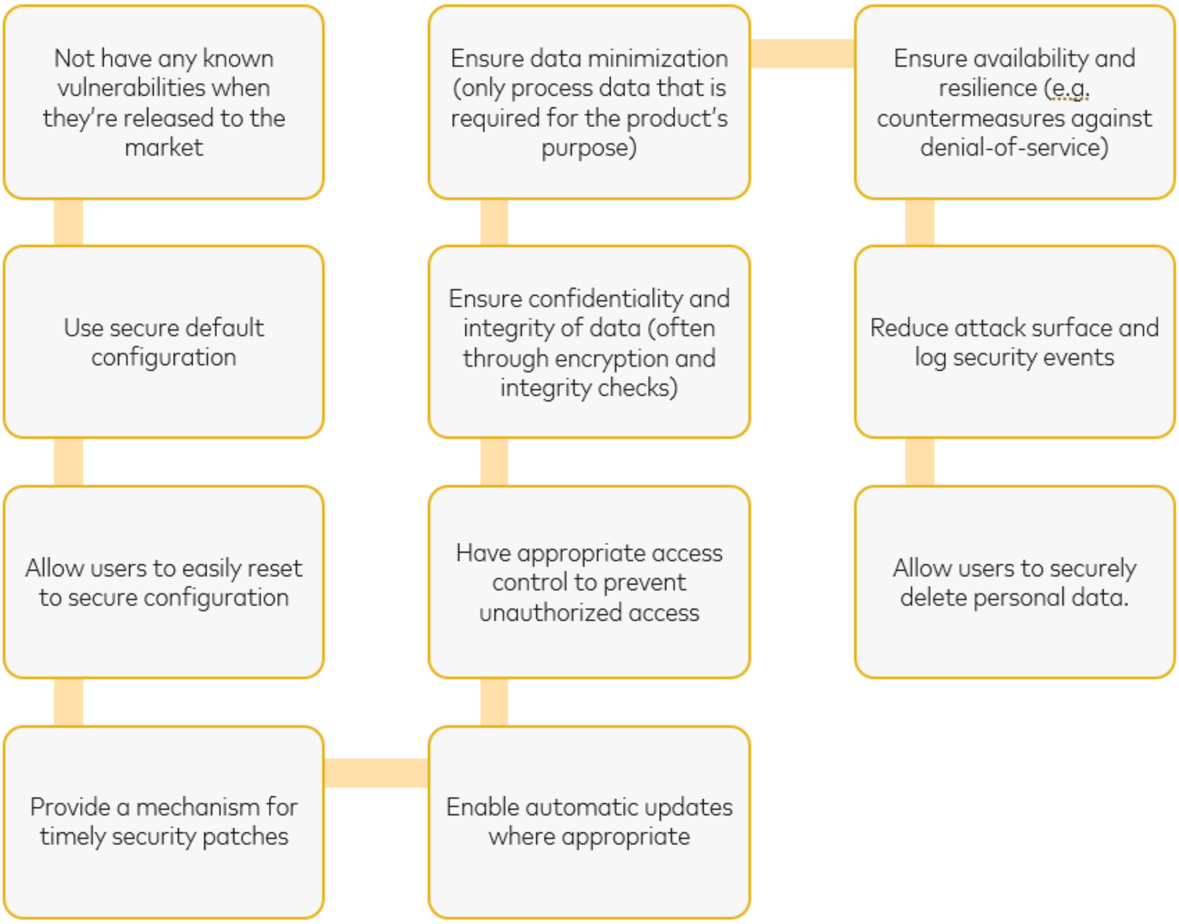
The manufacturers together with suppliers bear full responsibility for CRA obligations because they perform product design and construction and product maintenance functions. Product development engineers along with software developers need to practice secure coding methods to fulfill essential requirements. The essential function of Product Security Officers/Engineers (or a dedicated Product Security Incident Response Team) involves managing vulnerabilities and reporting incidents.

Companies establish a single contact point for vulnerabilities which functions as coordinator which receive and handles vulnerability disclosures. Tehe quality and compliance managers will develop the technical files needed while leading the product through the CE marking evaluation procedures. The corporate CISO provides guidance, but CRA compliance responsibilities mainly rest with R&D, product management and regulatory compliance teams. A hardware manufacturer needs their firmware developers together with product managers and compliance officer to create secure-by-design features while maintaining a software bill of materials (SBOM) and handling vulnerability disclosures with authorities.

Security Requirements

The CRA's Annex I defines "essentials cybersecurity requirements" for products, and they're much more detailed. Part I of Annex I focuses on the characteristics of the product and technical design mandates and includes such requirements as:

Figure 8: CRA Security Requirements


Not have any known vulnerabilities when they're released to the market
Use secure default configuration
Allow users to easily reset to secure configuration
Provide a mechanism for timely security patches
Ensure data minimization (only process data that is required for the product's purpose)
Ensure confidentiality and integrity of data (often through encryption and integrity checks)
Have appropriate access control to prevent unauthorized access
Enable automatic updates where appropriate
Ensure availability and resilience (e.g. countermeasures against denial-of-service)
Reduce attack surface and log security events
Allow users to securely delete personal data.

Annex I part II requires vulnerability handling process and manufacturers must have a coordinated vulnerability disclosure policy in place, keep a software bull of materials for their product's components, conduct security testing at regular intervals, and be able to provide security patches to users "without undue delay". Users must also be informed about vulnerabilities and fixes (e.g. advisory information should be published when patches are released). These requirements are in line with the best practices such as Secure Development Lifecycle and approaches (threat modeling, code review, pen-testing) and standards, such as ETSI EN 303 645 (security for IoT) or ISO/EIC 27034 (applications security).

Main Compliance Requirements & Actions

Key actions for manufacturers include:

- ✓ Carry out the product risk assessment at the design stage, ensuring that all necessary security measures are integrated into the product (according to Annex I) and compile a Technical Documentation file with evidence, such as test report, SBOM, risk assessment, etc.
- ✓ Go through a conformity assessment procedure before selling products into EU market. For the majority of "ordinary" products (which are not classified as highly critical) this will most likely be self-assessment where the manufacturer signs an EU Declaration of Conformity (official document that the product complies with CRA) and affixes the CE marking. Other product categories that fall under the higher risk categories will be required to have a notified body (independent auditor) confirm compliance.
- ✓ Put in place a maintenance and support process
- ✓ Specify and meet a support period for security updates
- ✓ Continuously check for vulnerabilities and fix them "without undue delay" throughout the product's life. Here the best practices include establishing a vulnerability monitoring team, subscribing to vulnerability databases and having patch development workflows in place.

Compliance with be an ongoing process – each product version may have to be re-checked, technical files revised, and new CE certificates issued in case of any significant changes. Internal audits and product pen testing on a regular basis can be seen as best practice to guarantee conformity. Manufacturers should also include CRA compliance in their current quality management system.

Reporting Obligations

CRA introduces mandatory reporting for product security issues: specifically, manufacturers must notify the authorities of any actively exploited vulnerability in their product and any incident that has a significant impact on the product's security.

The reporting will be done via a single European platform which will be managed by ENISA and will forward the reports to the relevant national CSIRT Coordinator and to ENISA at the same time. The timelines are very tight: an early warning must be submitted within 24 hours of the manufacturer learning of an actively exploited vulnerability or a serious incident, with at least preliminary info (and whether it's suspected to be from malicious attack). A fuller incident notification is due within 72 hours with an initial incident assessment an mitigation steps, and a final incident report within 1 month.

For vulnerabilities, after 24-hour warning, a follow-up vulnerability report is required within 72 hours (if more info is available) and a final remediation report no later than 14 days after a fix is available. These reports include details like the nature of the vulnerability/incident, which products are affected, what fixes or mitigations exist, and how sensitive the information is (to handle confidentiality).

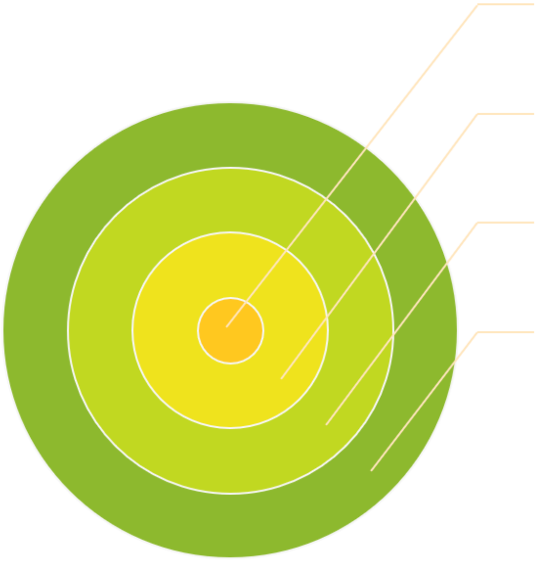
The CRA establishes an EU-wide vulnerability notification system: ENISA will use the information to inform other authorities and produce biennial trend reports. Notably, the Act is concerned with exploited vulnerabilities – manufacturers are only required to report bugs that are being used in the wild (or incidents that affect security) and not all bugs they discover. This ensures authorities get actionable intelligence (similar to how airlines report safety incidents). Manufacturers must also maintain a point of contact to report vulnerabilities.

The regulatory reporting is about notifying ENISA/CSIRT once a serious issue is confirmed. Additionally, if a product incident endangers user data or safety, manufacturers might also have to inform their customers/users. Though CRA doesn't explicitly force user notification, transparency is encouraged via disclosure of fixed vulnerabilities. In practice, compliance means having a Product Incident Response process which is part of the company's PSIRT and when a critical exploit is known, they must gather details and start the 24-hour clock. These templates will include technical information, IOCs, impact, etc.

Enforcement Mechanism

CRA will be enforced through the European Union's Product Compliance Framework. Each member state will designate market surveillance authorities (MSAs). Often these authorities are the existing Consumer Product Safety or Electronics regulators, now with cybersecurity added to their remit. These authorities have the power to request technical documentation, test products, and investigate whether the product meets CRA requirements. If a product is suspected to be non-compliant or poses a cybersecurity risk, MSAs can order corrective actions. For example, they can mandate the manufacturer to fix the non-compliance, recall or withdraw the product from the market, or halt further product sales. Market authorities will conduct surveillance campaigns and may target products randomly or based on incidents. The CRA also sets up an Administrative Cooperation Group (ADCO), where national MSAs coordinate enforcement strategies and exchange information. For instance, sharing SBOM data to perform "dependency risk assessments" across products. ENISA will operate the vulnerability reporting platform, but enforcement of remedies for those vulnerabilities lies with MSAs (they will know from reports if a vendor isn't patching timely, for example).

Figure 9: CRA Enforcement Ecosystem



Manufacturer

Direct Enforcement

Market Surveillance Authorities (MSAs)

Coordination and Support

- Administrative Cooperation Group (ADCO)
- ENISA

Cross-Domain & EU-Level Oversight

- Data Protection Authorities
- European Commission
- EU Cybersecurity Certification Framework (EU CSA)

There is an emphasis on cross-domain cooperation: MSAs should operate with data protection authorities for issues that overlap (like insecure products leading to personal data breaches). Also, the European Union Commission can intervene via a Union safeguard procedure if a particular product poses a serious risk EU-wide. This approach is similar to how dangerous toys or electronics are handled. Manufacturers must be prepared for compliance audits: MSAs can at any time request the products technical file and evidence of conformity. If the documentation is insufficient or the product fails security tests, enforcement actions follow.

There is also potential integration with the EU Cybersecurity certification framework (EU CSA). Although certification is voluntary, the CRA enforcement mechanism encourages using European cybersecurity certificates or harmonized standards as a demonstration of compliance. In summary, enforcement of the CRA will feel akin to how European Union enforces Product Safety today – with regulators empowered to ban insecure products and penalize manufacturers. This is a shift for cybersecurity: failure to secure a product can lead to it being pulled from markets.

Penalty Severity

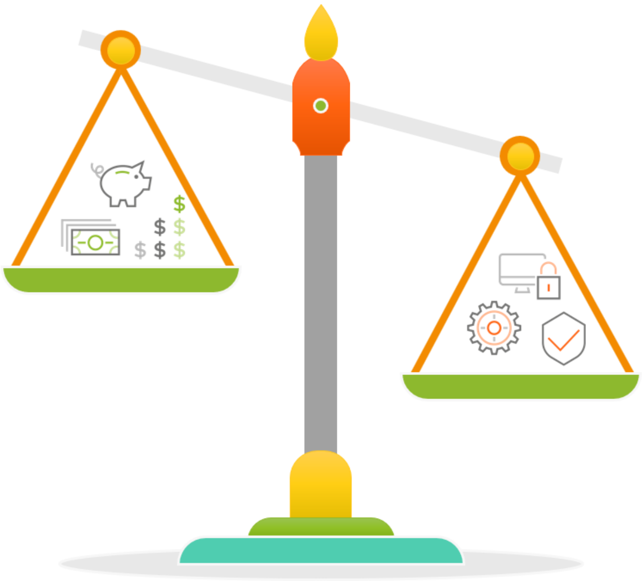
CRA sets out a three-tier fine structure for non-compliance:

1. For the most serious breaches, non-compliance with the essentials design requirements or the obligations of manufacturers to assess and report vulnerabilities/incidents - fines go up to €15 million or 2.5% of worldwide annual turnover, whichever is higher.
2. For other significant failures (such as not fulfilling obligations for other economic operators like importers, distributors or failing to meet documentation and transparency requirements, etc.) - fines up to €10 million or 2% of turnover can apply.
3. For lesser offenses (e.g. providing incorrect or misleading information to authorities or notified bodies) - up to €5 million or 1% of turnover.

These ceilings mean that, like NIS 2, CRI can hit large tech manufacturers with multimillion penalties, though again slightly lower than GDPR top 4%. The CRA also contemplates taking into account whether the offender is an SME or startup when deciding to find amount and encourages not double penalizing across multiple states for the same incident (which requires coordination via the info sharing system).

Apart from monetary fines, the big "penalty" under CRA can be the compliance actions themselves. For example, a vendor may be forced to recall products or issue updates under regulatory orders, which can be very costly operationally. Aside from fines, there is also damage to reputation, since regulators can make public announcements about insecure products. The prospect of 2.5% turnover fines is meant to be cybersecurity at the same board level attention that GDPR gave to privacy.

Figure 10: Enforcement Ecosystem



Comparative Analysis: NIS 2 and CRA

Criteria	NIS 2	CRA
Purpose	Strengthen cybersecurity resilience and continuity of critical services and infrastructures within the EU	Ensure products placed on the EU market are secure by design and by default, reducing cyber risks at the product level.
Scope and object	Medium and large entities in essential and important sectors (energy, health, finance, digital infrastructure, public administration, telecoms, etc.); SMEs included if vital nationally; certain digital services regardless of size	All manufacturers and vendors of digital products placed on EU market (consumer/industrial IoT, network devices, etc.); no SME exemption but special considerations for SMEs in enforcement. Open-source (non-commercial) exempt.
Level of regulation	Principle-based, flexible, risk-based governance requirements	Prescriptive, detailed cybersecurity requirements for products
Timelines	Transposition by Member States by October 17, 2024; compliance required immediately thereafter	Obligations phased in from mid-2026 (vulnerability reporting) with full product compliance required by mid-2027.
Affected roles	CISOs, risk managers, compliance officers, IT security teams, senior management accountable for compliance	Product developers, product security teams (PSIRT), compliance officers, engineering managers responsible for product lifecycle security
Security requirements	Broad organizational controls (risk management, business continuity, incident management, asset management, third-party security, staff training). Typically aligned to ISO 27001/NIST CSF.	Explicit technical requirements (secure defaults, encryption, secure updates, access control, data minimization, audit logging, SBOM, coordinated vulnerability disclosure, vulnerability management processes).
Main compliance requirements & actions	Organizational security measures implementation, incident reporting, continuous improvement, governance structures, audits, monitoring	Product risk assessments, compliance documentation, conformity assessment (CE marking), lifecycle management including ongoing vulnerability management and secure updates
Reporting obligations	Incident reporting to national CSIRT: early warning within 24h, detailed within 72h, final within 1 month. Inform affected users promptly.	Reporting actively exploited vulnerabilities/incidents to ENISA platform: initial notification within 24h, detailed follow-up within 72h, final remediation report within 14 days after fix.
Enforcement mechanism	Supervision by national cybersecurity authorities with power to audit, inspect, enforce, and impose corrective actions or fines. EU-wide coordination via cooperation groups and ENISA.	Market Surveillance Authorities (MSAs) perform conformity checks, test products, and enforce compliance via market bans, products recall, corrective actions, and fines. Coordination via EU-level groups.
Penalty severity	Essential entities: up to €10M or 2% turnover. Important entities: up to €7M or 1.4% turnover. Penalties are proportionate to violation severity.	Fines tiered: most severe violations up to €15M or 2.5% turnover, moderate violations €10M or 2%, minor €5M or 1%. Penalties proportionate, with SME considerations.

Overlaps and combined impact of NIS 2 and CRA

Complementary Scope

The NIS 2 and CRA have complimentary scopes, with one addressing services and organizations and the other – products and supply chain. There's a natural synergy: secure products (CRA's goal) should reduce the risk of incidents in the operators of essential services (NIS 2 domain). For instance, a hospital that is under NIS 2 will be safer if the medical devices it uses are built securely per CRA standards. In the strategic EU policy, these instruments are part of a cohesive approach (the EU Cybersecurity strategy): NIS 2 enhances the resilience of critical operators while CRA pushes cybersecurity upstream into the manufacturing of ICT products thereby increasing the baseline for everyone.

Information Sharing and Coordination

The laws explicitly acknowledge each other. The CRA reporting mechanism is linked to the NIS 2 ecosystem as ENISA will forward reports of product vulnerabilities to the NIS Cooperation Group and the relevant CSIRTs. Therefore, trends observed under CRA (e.g. a rise in IoT device exploits) can easily inform the NIS 2 authorities and sector regulators. In addition, the Cooperation Group under NIS 2 can discuss findings from CRA incident data in order to ensure that strategies for critical supply chains are properly aligned. On the other hand, if the NIS 2 authorities identify systemic product issues (for instance, a pattern of insecure SCADA components across energy operators), that intelligence can be fed into CRA enforcement priorities (for instance, MSAs may then target those products for compliance checks). This way, the frameworks of NIS 2 and CRA for cyber crisis management are linked and provide a more holistic view of cyber risk from product design to operational deployment.

Overlap of Targets

Despite their distinct focus, there is an overlap in who is affected. Several large tach companies will be subject to both regimes. For example, a cloud service provider is an essential entity in NIS 2, and if it also develops appliances and provides them to customers, it will also fall under CRA. This dual applicability means that such companies have to develop two compliance programs. Fortunately, there's alignment in underlying principles – risk management, security by design, continuous monitoring – so efforts can be synergistic.

Supply Chain and 3rd Party Risk

NIS 2 requires companies to assess supplier security, in effect creating demand for secure products – a synergy with CRA's supply of secure products. An essential entity under NIS 2 will most likely want CRA compliant products (and may even request CRA certification evidence in procurement). In that sense, CRA assists organizations in meeting their NIS 2 supply-chain duties by providing a baseline assurance on products.

Regulatory Complexity for Businesses

Businesses that both offer services and create products (common in sectors like tech, automotive, energy) will have to deal with multiple regulators, e.g. a smart grid company may have to interact with a NIS 2 authority for its energy operations and an MSA for its connected device products. It will be crucial for these regulators to be on the same page. The EU is trying to avoid contradictory obligations: the CRA contains clauses to avoid overlapping with sectoral laws that already have cybersecurity provisions (for example, if an automotive manufacturer complies with vehicle cybersecurity rules, that may count towards CRA compliance. In the same way, NIS 2 defers to sector-specific regimes like DORA for the financial sector (i.e. banks follow DORA primarily, not NIS 2, to prevent duplication). These guardrails against double regulation help, but companies will have to map out which rules apply to which parts of their business.

Main challenges introduced by NIS2 and CRA regulations for European organizations and others

The NIS 2 Directive and CRA represent a strategic regulatory expansion of European cybersecurity, but they introduce substantial difficulties at three levels: structural, operational and strategic.

The main structural difficulty emerges because the NIS 2 directive extends its regulatory coverage to more areas, such as energy, transport, banking, healthcare, digital infrastructure and water systems. The directive's expansion of regulated entities now reaches over 160,000 organizations throughout the EU, which creates substantial administrative challenges for national regulatory authorities. National regulatory authorities must now deal with extensive monitoring responsibilities of numerous organizations while lacking sufficient digital infrastructure alongside insufficient personnel and limited financial capabilities for efficient oversight. The processing of higher volumes of compliance requests and perimeter inclusion inquiries creates major operational difficulties which demand better technical capabilities and more agile processes together with robust digital platforms.

OVERLAPS AND COMBINED IMPACT OF NIS 2 AND CRA

Operational challenges affect smaller and medium-sized enterprises (SMEs) at a significant level. These organizations possess low cybersecurity maturity because they have historically spent minimally on security measures while keeping outdated systems without proper cybersecurity personnel or resources. The new mandate requires these organizations to quickly establish comprehensive cybersecurity governance systems together with risk management protocols incident response capabilities supply chain security measures and vulnerability management practices. The limited financial resources of SMEs force them to use essential cybersecurity tools like antivirus software and security outsourcing which leaves them unprepared for the detailed requirements of NIS 2 and CRA compliance. The lack of precise direction makes SMEs waste their resources while they solve individual compliance problems instead of developing their overall organizational cybersecurity capabilities. The CRA intensifies existing pressures by demanding secure-by-design requirements and lifecycle management standards for digital products which smaller firms have traditionally neglected.

The workforce deficit worsens operational problems while creating structural difficulties. Europe faces a severe cybersecurity professional shortage that reaches more than 200,000 available positions which affects both public institutions together with private organizations. Many organizations which face new compliance obligations do not have CISOs or compliance officers or incident response experts, so they assign their cybersecurity tasks to already overworked general IT staff. The operational risk becomes significant because organizations must detect incidents and repair vulnerabilities and fulfill the requirement for immediate notification within 24 hours.

The regulatory frameworks' push for digital transformation creates strategic challenges that were not directly anticipated. The process of digitization pushed by regulatory requirements can make SMEs and traditional non-digital sectors unintentionally increase their cybersecurity exposure when they add connected devices to their systems without proper infrastructure segmentation or employee training.

The European cybersecurity resilience depends on strategic investments that improve regulatory capacity and develop cybersecurity governance maturity alongside workforce development because NIS 2 and CRA provide fundamental security foundations. The effectiveness of these regulations depends on coordinated actions because regulatory requirements may exceed the implementation capabilities of less mature sectors and SMEs.

Building a Resilient Cyber System Across Europe

To address the growing demands of NIS 2, CRA, and adjacent regulations such as DORA and GDPR, the EU must shift from fragmented compliance to a cohesive model of cybersecurity infrastructure. This requires the synchronization of technical frameworks, enforcement mechanisms, and talent pipelines, enabling the public and private sectors to co-develop capabilities that are scalable, interoperable, and adaptable to evolving threats.

Consistency with Technical Frameworks

Building on the legal baselines set by NIS 2 and CRA, there is a pressing need to translate regulatory obligations into actionable operational standards. This includes interoperable incident response playbooks, aligned risk assessment criteria, and sector-specific guidance on supply chain security and vulnerability handling.

ENISA should continue leading in this domain by expanding its portfolio of implementation guidelines, scenario-based exercises, and best practice libraries to cover not only mature sectors like finance and energy, but also emerging ones like health tech and municipal services. Harmonized baseline standards such as the adoption of ISO/IEC 27001, the NIST Cybersecurity Framework, or ETSI EN 303 645 will help streamline implementation and reduce the burden on organizations navigating multiple overlapping regulations.

Collaborative Threat Intelligence Platforms

A resilient cybersecurity infrastructure must be supported by federated, near-real-time threat intelligence exchange that spans national boundaries and industrial domains. While mechanisms such as ISACs (Information Sharing and Analysis Centres) and CSIRTs already exist, they often operate in isolation, use incompatible formats, or lack scalable governance.

To improve threat visibility and response times, the EU should support the development of standardized, trusted exchange protocols that allow anonymized yet actionable data sharing across sectors. CRA's mandatory vulnerability reporting and ENISA's coordination role can serve as key inputs into a pan-European situational awareness platform, enabling early detection of systemic risks.

Investment in Cross-border Infrastructure and Capabilities

The implementation of CRA and NIS 2 cannot succeed without tangible investments in shared cybersecurity infrastructure, particularly for Member States and sectors with lower maturity levels. EU funding programs like the Digital Europe Programme and Horizon Europe should prioritize:

- ✓ The creation of regional Security Operations Centres (SOCs) and cyber crisis response hubs;
- ✓ Expansion of joint cyber exercises, modeled on those already piloted in the energy and financial sectors;
- ✓ Public-private labs for secure software development and vulnerability research.
- ✓ Stress tests - such as those conducted on energy infrastructure in 2023 - should be extended to other critical verticals like transport, telecommunications, and healthcare, with ENISA coordinating sector-specific methodologies.

Embedding Resilience by Design at Infrastructure Level

While the CRA mandates secure-by-design practices for digital products, this principle must also extend to procurement, configuration, and maintenance of broader IT and OT infrastructure. Member States should adopt CRA-aligned procurement policies and incentivize organizations to choose certified or compliant products where available, especially under the EU Cybersecurity Certification Framework4.

Additionally, zero-trust architectures, continuous security monitoring, and asset visibility tools should be promoted as foundational elements of national digital infrastructure programs. Resilience must be engineered not only into products but into the systems and networks that deploy them.

Capacity Building and Public-Private Cooperation

A resilient ecosystem requires skilled people not just systems. The cybersecurity talent gap is among the EU's most critical vulnerabilities. To close this, the EU should:

- ✓ Expand cybersecurity education, vocational training, and re-skilling programs at both national and EU levels;
- ✓ Support local cyber hubs or "cyber clinics" to assist SMEs with NIS 2 and CRA compliance;

- ✓ Launch a European Cyber Workforce Initiative with incentives for cross-border mobility and public-private secondments.

Public-private collaboration should also extend to the regulatory side. Member States and EU agencies must equip their national regulators with shared toolkits, reporting platforms, and audit templates to scale up oversight efforts. The NIS Cooperation Group and ADCO (Administrative Cooperation Group under CRA) can facilitate this harmonization, ensuring that audit burdens are shared and enforcement remains consistent across jurisdictions.

How Mastercard can support in the journey to the compliance with NIS 2 and CRA regulations

The journey toward compliance with NIS 2 and CRA typically follows a structured, multi-phase process. Mastercard has developed its own methodology to support organizations in the alignment with Cybersecurity-related requirements stated by those regulations.

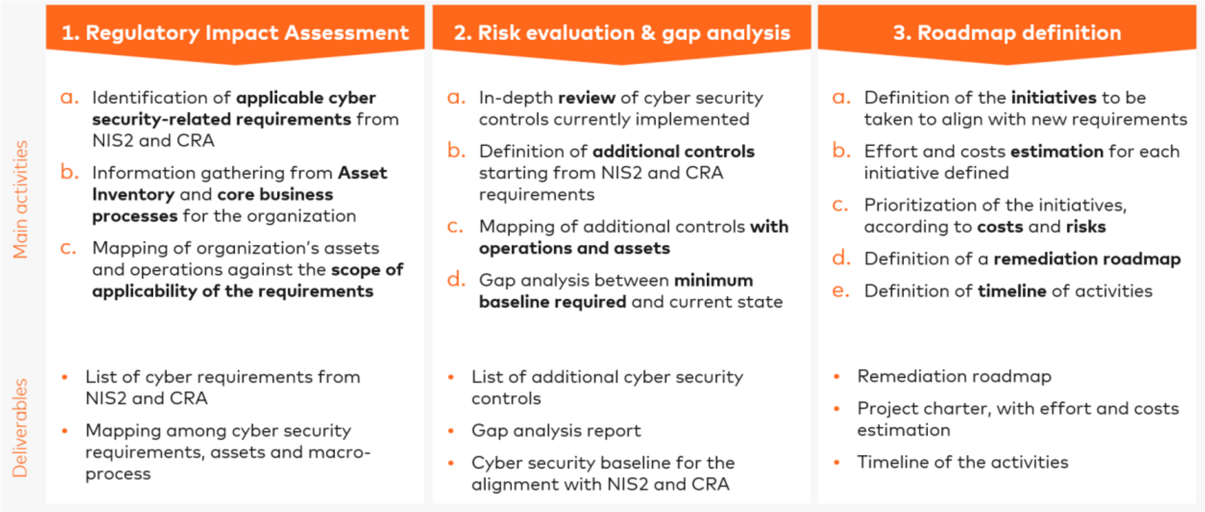
As a first step, our Strategy & Transformation consultants begin by conducting a regulatory impact assessment. This step involves mapping the organization's operations, digital assets and dependencies against the scope and applicability of the new requirements. Indeed, under NIS 2, organizations must evaluate whether they qualify as "essential" or "important" entities, a distinction that dictates the depth of their obligations. Similarly, the CRA mandates a review of software and hardware products to determine whether they fall under the regulation's categories, such as "critical" or "non-critical" digital products.

Once applicability is established, the next phase involves risk assessment and gap analysis. Mastercard performs in-depth reviews of existing cybersecurity measures, policies and incident response mechanisms to identify shortfalls related to NIS 2 and CRA requirements. This includes evaluating technical safeguards, such as Network Security, Access Control and encryption, as well as Governance aspects like Cyber Risk Management frameworks, Supply Chain Security and Business Continuity & Disaster Recovery planning. In order to do so, Mastercard relies on its Cybersecurity experts, that may leverage multiple tools to both automate risk evaluation phase and provide more detailed results than through any manual process. Cyber Quant is the Mastercard product for cyber risk quantification: it is able to identify, assess and evaluate risks starting from the answers provided by organization's personnel to questionnaires and cyber threat intelligence data collected autonomously; the outcome is reported under the form of qualitative indicator for risk and economic quantification of potential financial loss in case one or more risk scenarios will become reality.

Besides risk evaluation and quantification, Cyber Quant is able to provide also recommendations on how to address the main gaps identified during the assessment phase. Gaps are mapped with cybersecurity control areas in accordance with the framework in use, which may reflect one or more standards and regulations; recommendations are actionable and tailored to the organization's architecture.

Following the identification of gaps, Mastercard consultants work closely with internal stakeholders to develop a remediation roadmap. This roadmap outlines prioritized actions, resource allocation and timeline for achieving full alignment with NIS 2 and CRA.

Figure 11: Mastercard Approach to NIS 2 and CRA Alignment



	1. Regulatory Impact Assessment	2. Risk evaluation & gap analysis	3. Roadmap definition
Main activities	a. Identification of **applicable cyber security-related requirements** from NIS2 and CRA b. Information gathering from **Asset Inventory** and **core business processes** for the organization c. Mapping of organization's assets and operations against the **scope of applicability of the requirements**	a. In-depth **review** of cyber security controls currently implemented b. Definition of **additional controls** starting from NIS2 and CRA requirements c. Mapping of additional controls **with operations and assets** d. Gap analysis between **minimum baseline required** and current state	a. Definition of the **initiatives** to be taken to align with new requirements b. Effort and costs **estimation** for each initiative defined c. Prioritization of the initiatives, according to **costs** and **risks** d. Definition of a **remediation roadmap** e. Definition of **timeline** of activities
Deliverables	• List of cyber requirements from NIS2 and CRA • Mapping among cyber security requirements, assets and macro-process	• List of additional cyber security controls • Gap analysis report • Cyber security baseline for the alignment with NIS2 and CRA	• Remediation roadmap • Project charter, with effort and costs estimation • Timeline of the activities

Mastercard may guide the deployment of appropriate cybersecurity tools, or the review of existing policies, processes and procedures.

As compliance is not a one-time effort, Mastercard also helps organizations in designing continuous monitoring and reporting mechanisms. This includes the definition of Key Performance Indicators (KPIs), Key Risk Indicators (KRIs) and periodic internal auditing calendar.

It is highly recommended that a periodic re-evaluation of cyber risks and gap analysis is conducted during the implementation of remediation roadmap, in order to double check that cyber risks are effectively mitigated by the implementation of the new cybersecurity measures or the improvement of the existing controls. The use of Cyber Quant may ensure that evaluation criteria remain the same for the whole implementation phase. On top of that, Cyber Front could be run to verify the effective roll-out of new solutions; this is a Breach and Attack Simulation tool, aiming at testing and measuring the ability of organizations' security controls to defend against the latest threats.

The execution of technology-based tests may serve to crack bias in organizations and gather concrete evidence about the effectiveness of the tools adopted.

Conclusion

Cybersecurity represents a key priority for Mastercard; recent acquisitions and the attention of the company towards the new regulations and the shifts in the cyber threat landscape have led to remarkable investments to align its internal systems first and then shape a consistent offering for its customers. NIS 2 and CRA represent another milestone in this path to strengthen the resilience of the business.

Solutions based on solid tools and consulting services, provided by an expert network of Cybersecurity Subject Matter Experts (SMEs), have been developed and brought into several discussions with customers.

Success stories can be found in different countries across Europe, with projects connected to NIS 2 that are taking place in Ireland and Germany; moreover, in Austria, Italy, Croatia and Romania there are opportunities under discussion. Due to the vast scope of applicability of NIS 2, and due to the robust proposition on this topic, Mastercard is building strong references in industries such as Accommodation, Dining, Healthcare, Public and Tourism.

Regarding CRA, Mastercard is trying to bring its innovative approach to clients in the Italian market, belonging to specific sectors (e.g., Gaming, Betting).

Contact us to learn how Mastercard's Enterprise Cybersecurity Platforms support the full ecosystem resilience cycle with Cyber Insights, Cyber Quant, RiskRecon, Cyber Front, Cyber Crisis Management, and Threat Protection.

Contributors

Alessandro Miracca
Advisory Client Services
Mastercard

Süheyl Hamavioğlu
Product Management
Mastercard

Karina Dalhunova
Product Management
Mastercard

Coordinator

Eda Boltürk, Ph.D., Assoc. Prof
Product Management
Mastercard

References

Figure 1, page 3
Mastercard Cyber Insights Data

Scope and Object of Regulation, page 5
Infosecurity Europe