bitkom

Position paper

August 2026

CRA: 15 Scenarios for Economy, Market, and Supply Security

The Cyber Resilience Act is a significant step for Europe's cybersecurity. It sets binding minimum requirements for products with digital elements EU-wide and strengthens "Security by Design." The digital economy explicitly supports this goal: Higher cybersecurity standards protect companies, citizens, supply chains, and critical infrastructure.

At the same time, the CRA is an industrial policy milestone, whose impact depends on successful implementation. This requires clear standards, robust guidelines, sufficient testing and certification capacities, as well as harmonized market supervision. Conformity assessment bodies must early on develop testing procedures, personnel, accreditations, and a uniform level of testing; otherwise, there is a risk of a structural bottleneck. The administrative additional burden should be manageable, and associated additional costs must be minimized.

Currently, there are significant implementation gaps. Companies are preparing for December 2027, even though harmonized standards, delegated acts, interpretation aids, certification procedures, and market supervision requirements are lacking. At the same time, non-compliance could result in sanctions or loss of market access. This affects companies of all sizes.

The European Commission, the federal government, the BSI, and the responsible accreditation body should prioritize implementation much more strongly. Early available standards, viable testing capacities, clear contacts, and a uniform supervisory practice are necessary. If regular listing of the relevant harmonized standards is no longer possible by 11 December 2026, a two-year transition period should be allowed between their publication in the EU Official Journal and their initial application. The goal must be to enhance cybersecurity without impairing innovation, product availability, and competitiveness through avoidable uncertainties.

This paper describes concrete risk scenarios from the economy's perspective and thus complements the basic Bitkom demands for the CRA. The scenarios show the practical consequences that can arise if central implementation questions remain unresolved by December 2027.

1. Product variants, changes, and product life cycles

Scenario 1: Disproportionate individual assessment of customer-specific UICC/SIM variants

Initial Situation

SIM cards fundamentally consist of a hardware chip, operating system, and network profile. Mobile network operators regularly define their own variants, which are customized by the manufacturer based on a general operating system and identical hardware. These variants usually do not contain additional functions but are restricted versions of the general operating system. Therefore, a particular SIM card product can only be delivered to the mobile network operator who specified it.

CRA Challenge

Under the CRA, comprehensive conformity assessments would become necessary for UICC/SIM products. If customer-specific variants are certified separately, significant additional costs arise for manufacturers and notified bodies. These costs become a structural fixed cost driver: providers with high production volumes can spread them across larger quantities, while smaller providers and new market entrants find it significantly harder. Particularly at low initial volumes, CRA-related certification costs can become a significant economic hurdle.

Possible Consequence

This may lead to market distortions and a greater concentration on a few large providers. Mobile network operators might concentrate procurement volumes further on the cheapest provider for cost reasons. Smaller manufacturers would need to evaluate whether certifications still make economic sense with low quantities; new providers would face much higher market entry hurdles. A reduced provider landscape can weaken the resilience of European supply chains. In the event of production outages, CRA-relevant vulnerabilities, recalls, or mandatory security updates from a large provider, several mobile network operators and downstream areas could be affected simultaneously, such as mobile communications, IoT applications, connected vehicles, or industrial applications.

Improvement Proposal

CRA conformity should be provable for a general operating system and easily transferable to derived customer-specific variants, provided they do not contain functions beyond the verified scope. This could significantly reduce the certification effort without lowering the CRA's security level. Simultaneously, notified bodies would be relieved, testing capacities used more efficiently, market entry barriers limited, and the diversity of providers preserved.

Scenario 2: Lack of certification foundations for smartcards and secure elements

Initial Situation

Smartcards and Secure Elements form the security foundation of numerous critical applications and global infrastructures, such as in payment, mobile communications, healthcare, passports/identity cards, identity management, as well as authentication and access control systems. Thus, they directly contribute to the security goals of the CRA. The products are often used over long periods and rely on highly specialized hardware, operating systems, and application components.

CRA Challenge

Specific and recognized CRA standards for these complex and safety-critical components are currently lacking. Corresponding standards are still in development and are not expected to be available before spring 2027, while vertical-specific standards (e.g., Protection Profiles) will take even longer. Preparation, testing, and evaluation for smartcards require at least a comparable lead time as established Common Criteria processes. Additionally, retrospective certification of (existing) products that have not previously been certified is either impossible or involves significant effort. Without early available, binding, and product-specific guidelines, manufacturers lack the necessary planning and investment security.

Possible Consequence

Manufacturers might discontinue smartcard solutions if their CRA compliance cannot be economically proven or achieved within the remaining time frame. A like-for-like replacement is not readily available for many custom applications. As a result, solution providers might resort to more easily assessable but less secure pure software solutions or forgo hardware security elements, effectively lowering the security level contrary to CRA objectives. Necessary redesigns are simultaneously under significant time pressure and tie up resources needed for technical advancement.

Improvement Proposal

Established certifications like EUCC, existing Common Criteria evaluation reports, and existing quality processes based on ISO 9001 should be recognized and reused as the foundation for CRA compliance assessment. Additionally, modular approaches such as product family or "umbrella" evaluations are needed so that not every technical variant has to be completely reevaluated. The European Commission and relevant authorities should publish technology-specific requirements, Protection Profiles, and reliable transitional rules at an early stage. Long-used certification schemes in the industry, which have demonstrably ensured a very high, equivalent security level, must be appropriately recognized, for example by creating specific CSA schemes and recognition procedures for them. An anticipated, unmanageable flood of recertifications must be avoided. Therefore, sufficient transition periods should be defined in all cases.

Scenario 3: Re-evaluation Risks with Configurable Remote Maintenance Software

Initial Situation

Secure remote access and maintenance solutions allow controlled and logged access to systems in industries like industry, energy supply, healthcare, public administration, and other sensitive environments. These products often consist of a security-relevant product core that is adapted to their respective operational environments. Differences include deployment models, authentication, rights management, logging, and system integration. These configurations don't necessarily alter the product core but are crucial for secure operations.

CRA Challenge

For key products with digital elements, a third-party assessment by a notified body may be required. It's particularly unclear whether customer-specific configurations, changes in deployment models, or security-relevant updates trigger a new or supplementary compliance assessment. This question arises regularly with remote maintenance solutions, even though adjustments often only involve integration into the respective operational environment and don't alter the security-relevant product core.

Possible Consequence

Manufacturers might delay customer-specific integrations or hardening measures to avoid triggering unclear re-evaluation obligations. Consequently, users might have to work longer with less suitable or less hardened configurations. This impacts especially small and specialized providers with varied configuration models. If every adjustment becomes a potential evaluation risk, it favors standardized products from large providers, which could weaken diversity and resilience in a security-critical access layer.

Improvement Proposal

CRA compliance should be demonstrable at the level of a clearly defined product core or product family. Customer-specific configurations and deployment models should be covered by this assessment as long as they do not significantly alter or undermine the evaluated security scope. The European Commission should publish clear criteria and practical examples for changes that trigger re-evaluation.

Scenario 4: Re-evaluation Obligations in Continuous Software Development

Initial Situation

Modern software is continuously being developed. Security updates, bug fixes, and functional enhancements are often carried out in short development cycles through continuous integration, continuous deployment, and agile development methods. Changes are therefore not exceptional but an integral part of the regular development and security process.

CRA Challenge

For pure security updates, the European Commission's CRA Guidance provides more clarity: they are generally not considered substantial changes if they reduce cyber risk and do not alter the intended use. However, the distinction remains relevant for functional changes and combined releases in continuous development processes. Manufacturers must regularly evaluate whether new or altered functions change the intended use or the cybersecurity risk profile, necessitating a new or supplementary compliance assessment. In short release cycles, this case-by-case evaluation can add additional documentation and assessment workload.

Possible Consequence

Manufacturers might bundle functional changes more significantly or extend release cycles to limit the effort of repeated assessments. Especially small and medium enterprises might postpone functional advancements to restrict the effort of repeated compliance evaluations. This ties up development resources, stifles innovation, and can hinder the continuous development of products.

Improvement Suggestion

The existing criteria for substantial changes should be further operationalized for continuous software development. Changes that do not significantly alter the intended purpose and the cybersecurity risk profile, and maintain or improve the security level, should not trigger a renewed full compliance assessment. In addition, practical guidelines with further examples are needed, particularly for functional changes and combined releases in continuous integration and continuous deployment processes.

Scenario 5: Reassessment Obligations Jeopardizing Spare Parts Supply

Initial Situation

Products with digital elements often rely on a reliable supply of spare parts for many years. The required components are often specifically developed for a particular product. During the product lifecycle, changes may become necessary, for instance, because original components are no longer available or technical improvements need to be implemented. The causes don't always lie within the manufacturer’s control.

CRA Challenge

Spare parts with digital elements are generally exempted from the requirements of the CRA. However, according to the European Commission's CRA interpretation, this exception may cease to apply if a spare part is substantially changed. Proving full CRA compliance might then incur significant costs. For specialized spare parts with low production volumes, these often do not economically justify the actual security risk of the change. Even assessing whether a change triggers a CRA obligation ties up resources and leaves a legal and liability risk behind.

Possible Consequence

Manufacturers might forgo necessary adjustments or completely cease the provision of individual spare parts. Consequently, existing products could become prematurely unusable, although their actual cybersecurity is not compromised by the changed spare part. If spare parts production ends, resuming it later might be associated with significant costs or become technically impossible. This affects reparability, product lifespan, and supply security without providing a corresponding security gain.

Improvement Suggestion

Changes to spare parts should not trigger a renewed CRA compliance assessment as long as they serve to maintain availability or provide technical improvements, do not significantly alter the intended purpose, core function, and assessed safety scope, and do not degrade the security level of the overall product.

Scenario 6: Free Security Updates in Individually Agreed B2B Support Models

Initial Situation

Manufacturers of complex enterprise software typically support only a few product versions in parallel for stability and compatibility reasons. Enterprise customers often operate these solutions on-premises or in hybrid environments and especially in regulated industries, they rely on long validation and upgrade cycles. The basis is individually negotiated support and maintenance contracts. These regularly include security patches as well as compatibility checks, validations, deployment planning, service level agreements, lifecycle management, and hotfix engineering.

CRA Challenge

The CRA essentially obligates manufacturers to provide security updates promptly and free of charge. It is unclear if individually negotiated support contracts for highly configurable enterprise software fall under the exception for custom-made products with digital elements. Otherwise, manufacturers would either have to maintain legacy versions separately or enable a transition to newer versions for free. Both go distinctly beyond providing a mere security patch. It is also unclear how far the manufacturer's responsibility extends if an appropriate security update has been provided, but the operator cannot implement it due to compatibility requirements, approval processes, or their legacy environment.

Possible Consequence

Resources would be shifted from current product lines to maintaining historical versions. Manufacturers might shorten support periods and reduce the number of supported versions. Especially in regulated industries, customers might remain on older versions even when a security update is available. Without clear delineation of responsibilities, additional liability and compliance uncertainties arise. Meanwhile, there are disincentives for proactive vulnerability research, if findings on legacy versions trigger additional backport obligations. Cloud and subscription models would be structurally less affected than on-premises and hybrid-provided solutions.

Suggested Improvement

The concept of a customized product with digital elements should also encompass highly configurable enterprise software that is custom-integrated and operated on-premises or in a hybrid manner. If this clarification is insufficient, the word "customized" should be removed from Annex I as part of a Digital Omnibus to clarify that the cybersecurity objectives of the CRA can be fully achieved without limiting contractual agreements, freedom of choice, and technology-neutral business models. Furthermore, it should be clearly delineated which obligations remain with the manufacturer and which responsibilities lie with the operator when an appropriate security update has been provided but cannot be installed due to the specific operational environment.

Scenario 7: Disproportionate CRA Obligations for Low-Risk Mass Products

Initial Situation

The CRA also applies to simple peripheral communication devices, such as computer mice, keyboards, or webcams. These devices have a physical or logical data connection and thus use a digital element. However, the required driver is often not product-specific nor part of the device, but a device-independent HID driver already installed on the computer. Therefore, the product-specific security risk for such devices is generally limited.

CRA Challenge

IT peripherals are often marketed by trading companies that outsource development and production to external providers. These companies often lack the technical expertise and internal structures to independently and legally assess the cybersecurity risks of simple mass products. Although the CRA allows for internal conformity assessments for products with low security risk, without clear criteria and practical guidelines, it remains uncertain what tests and verifications are required.

Possible Consequence

To avoid liability and sanction risks, many companies may contract external testing bodies despite the low product risk. This would tie up existing testing capacities with products of low criticality and could lead to bottlenecks for genuinely security-relevant products. The resulting fixed costs particularly impact SMEs and specialized providers, who can only distribute additional compliance costs to a limited extent over large volumes or extensive customer bases. Individual products may become uneconomical and disappear from the European market without any corresponding gain in cybersecurity.

Suggested Improvement

The European Commission should exempt well-defined, inherently secure product groups from CRA requirements and provide simplified verification procedures for products with limited risk. This should include standardized self-declarations and preferably automated testing procedures; existing certifications and test reports should be reused as much as possible. Practical guidelines for internal conformity assessment under Article 32 CRA should establish clear testing criteria for this purpose.

2. Supply Chains, Components, and Vulnerability Management

Scenario 8: Vulnerability Reporting and Remediation in Multi-Tier Supply Chains

Initial Situation

Supply chains in the consumer electronics industry are often multi-tiered. Production partners either develop their own software or source components from additional suppliers. As a result, smart home products, for instance, can contain software components originally developed by several different companies. With each additional supply chain tier, the availability and transparency of the information required by European manufacturers for vulnerability management decrease.

CRA Challenge

Several supplier levels often exist between the European manufacturer and the original software developer, without a direct economic or contractual relationship. If a vulnerability is discovered, information still needs to be exchanged across the entire supply chain within short deadlines. The European manufacturer relies on the cooperation of all upstream suppliers but can only control this to a limited extent.

Possible Consequence

Obtaining complete Software Bills of Materials involves significant effort for many product groups. Individual upstream suppliers may be unable to provide a complete SBOM, perform vulnerability analyses on time, or make necessary security updates available. As a result, reporting and response deadlines can effectively become impossible to meet. European marketers face substantial liability and recall risks, even though the affected software was developed outside their company. In the extreme case, a product recall may be the only risk mitigation measure left.

Suggested Improvement

When applying reporting and response deadlines, it must be considered whether manufacturers can receive the required information from upstream suppliers in a timely manner, despite reasonable and documented efforts. Guidelines should specify which risk-mitigating interim measures are recognized when vulnerability information or security updates from upstream supply levels are not yet available. For clearly defined products with limited cyber risk, simplified SBOM documentation should also apply.

Scenario 9: Unclear CE marking for software and embedded components

Initial Situation

The CE marking is new for software, while it is already established for hardware products. Semiconductors and other embedded components are integrated in large numbers into complex end products. Once installed, they are not regularly accessible or visible to consumers. The conformity of the individual component is documented to customers and market participants through the EU Declaration of Conformity, while the finished end product carries its own CE marking. Semiconductor manufacturers also often have extensive product portfolios with numerous variants and configurations. For software, on the other hand, the CE marking represents a new requirement that needs further clarification, especially regarding the form and location of the marking.

CRA Challenge

Article 30 CRA regulates the application of the CE marking on products with digital elements. However, it remains unclear how to apply the requirements in certain situations for software and small or complex-shaped hardware products. For semiconductors, a physical marking also causes significant administrative burdens and is partially barely readable due to the small product size. After integration into an end product, it regularly offers no additional informational value to consumers.

Possible Consequence

Unclear requirements can lead to different interpretations and thus to formal non-compliance. At the same time, manufacturers would have to carry out extensive labeling and product modification processes, even though a physical marking of embedded components is no longer accessible after installation. The additional burdens tie up significant resources, especially during the transition, without correspondingly improving market surveillance or consumer protection.

Improvement Suggestion

The European Commission should clarify in its FAQs or CRA guidelines how the CE marking should be practically applied for software and for small or complex-shaped hardware products. Semiconductor and other embedded component manufacturers should be able to optionally place the CE marking in the EU Declaration of Conformity instead of on the individual component if marking the product is not practical due to its size, readability, or integration into an end product. In conjunction with the end product's CE marking, conformity would remain transparently documented.

Scenario 10: Double reporting obligation for actively exploited vulnerabilities and severe security incidents

Initial Situation

Article 14 CRA imposes reporting obligations for both actively exploited vulnerabilities and severe security incidents. In practice, both categories can be interconnected: the active exploitation of a vulnerability in a product can simultaneously cause a severe security incident.

CRA Challenge

It is unclear how manufacturers should handle an event that fulfills both criteria simultaneously. It is particularly ambiguous whether reporting the actively exploited vulnerability suffices if it is the immediate cause of the security incident, or whether a separate report of the severe security incident is also required. Since different information may be required for both reporting channels, manufacturers lack sufficient legal certainty regarding the scope and form of the report.

Possible Consequence

Manufacturers might be cautious and report the same event multiple times to avoid the risk of formal non-compliance. This leads to additional administrative effort and potentially duplicate or differing information being provided to the relevant authorities. Conversely, a single report risks being retrospectively deemed incomplete.

Improvement Suggestion

The European Commission should establish clear guidelines in its FAQs or CRA guidelines on how to handle cases where an actively exploited vulnerability simultaneously causes a severe security incident. A joint or clearly linked reporting process should be enabled when the cause is identical. It should be clearly defined which deadlines and information requirements apply to avoid duplicate reports and formal compliance risks.

Scenario 11: Missing supplier evidence for CRA compliance

Initial Situation

Products with digital elements are often created in multi-tiered supply chains with divided labor. Manufacturers source specialized hardware and software components from direct suppliers, who in turn depend on other upstream suppliers. Therefore, the technical information relevant for the final product resides with various players along the supply chain.

CRA Challenge

To demonstrate their own CRA compliance, manufacturers need reliable information and proof regarding the supplier products used. However, they cannot independently verify complex components in every case. Especially with specialized supplies, they often lack the technical skills or necessary information for their own inspections. Even if suppliers implement CRA requirements, the necessary evidence may only become available shortly before the effective date. In multi-tiered supply chains, time pressure intensifies. Individual suppliers, particularly outside the EU, may not provide sufficient evidence or may not align with European requirements.

Possible Consequence

Incomplete or delayed supplier information can significantly hinder or practically render impossible the proof of CRA compliance. Manufacturers might be forced to refrain from making products available despite their own preparations or to urgently seek alternative suppliers. The risk of regulatory failures would thus lie with companies that can only influence the lack of cooperation within their supply chain to a limited extent.

Improvement Proposal

Manufacturers should be given adequate time to review supplier information and incorporate it into their compliance assessment. Guidelines must establish how to deal with late, incomplete, or unavailable evidence despite reasonable efforts. Additional transition periods should be provided for particularly complex and multi-tiered supply chains if the manufacturer has thoroughly documented their procurement and inspection measures.

Scenario 12: Lack of Proof and Accountability Structures for Open-Source Components

Initial Situation

Modern software products are regularly composed of numerous internally and externally developed components. These often include hundreds or thousands of dependencies from open-source software. The individual components are developed under different organizational structures and maintenance models and subsequently integrated into many commercial products.

CRA Challenge

Manufacturers have to take responsibility for open-source components that they integrate into their products. However, unlike traditional supplier relationships, there is no contractually obligated party from whom manufacturers can demand security proofs, vulnerability information, or long-term updates for many of these components. Replacing all libraries or conducting extensive individual security assessments is practically unfeasible given the number and complexity of dependencies. Additionally, manufacturers may not have the necessary expertise for every component, particularly in security-critical areas like cryptography. Open-source software stewards can partially fill this gap.

Possible Consequence

Without reliable verification paths, manufacturers must evaluate numerous open-source components themselves, even though they may lack resources, information, or expertise. A complete examination of every individual library is hardly realistic for complex software products. As a result, manufacturers might forgo using proven open-source components or stop providing products economically. At the same time, additional regulatory obligations might deter potential stewards and weaken existing accountability structures.

Improvement Proposal

Risk-based, standardized, and as automated as possible testing procedures should be developed for widespread standard libraries. Passing such procedures should establish a presumption of compliance or be appropriately considered in compliance assessments. For components with increased security risks, practical supply-chain risk management models and clearly assigned responsibilities should be provided. Additional testing obligations should focus on particularly critical libraries and components.

3. Missing Preconditions for CRA Application

Scenario 13: Harmonized Standards Available Too Late

Initial Situation

Technical standards establish common criteria for product design, testing procedures, and proof of conformity, serving as central references for manufacturers, testing bodies, market surveillance authorities, and customers. Harmonized standards can also create a presumption of conformity.

CRA Challenge

For numerous CRA requirements, the relevant standards are still under development, including the ETSI-EN series and the 40000 standard series. According to the latest draft of the standardization request dated July 7, 2026, essential standards are expected to be published between October 2026 and October 2027. Additional delays cannot be ruled out. Although harmonized standards are legally voluntary, they are practically used as authoritative references by market surveillance authorities, testing bodies, and customers. Therefore, companies must either wait for the final standards or implement preliminary drafts that may change upon publication.

Possible Consequence

The late availability of standards significantly shortens the time frame for their practical implementation. Especially for complex products, long development cycles, and extensive product portfolios, full adaptation by the time of enforcement may be barely or no longer achievable. Companies face delays in conformity assessments, additional development costs, and legal uncertainty, despite the necessary reference requirements not being established in time. A too late publication of the standards along with limited certification capacities can also disrupt the supply of, for example, safety-relevant digital base components and thereby affect critical infrastructures.

Improvement Proposal

The period between the publication of key harmonized standards and the initial obligation to comply with the corresponding requirements must be sufficiently long. If it is no longer possible to list the relevant harmonized standards through the regular procedure by December 11, 2026, a two-year transition period should apply from their publication in the Official Journal of the European Union. During this time, products of the standard category and those in classes I and II should still be assessed based on the manufacturer's self-declaration according to Module A.

Scenario 14: Insufficient Capacity of Notified Bodies

Starting Point

The CRA provides for different paths of conformity assessment depending on the product category. For important and critical products with digital elements, an assessment by an independent notified body may be required. These bodies must be designated and accredited before commencing their activities, and must build the necessary technical and organizational assessment capacities.

CRA Challenge

The development of these structures has not progressed sufficiently. Currently, only a few bodies designated for CRA are available, while designation, accreditation, and capacity building require significant lead time. With the effective date approaching in December 2027, a sharp increase in demand is expected. There is, therefore, a risk that the demand for conformity assessments will rise much faster than the available supply. Even applications submitted early offer no guarantee that an assessment will be completed in time.

Additionally, the CRA is product-specific. For product series and advanced product generations, this can mean that new series of already established legacy products must also be reassessed for CRA conformity. This creates a continuously significant additional assessment demand. The demand for notified bodies could thus far exceed the already expected peak of transition.

Possible Consequence

Long waiting times could particularly affect small and medium-sized enterprises and manufacturers with low production volumes. They risk being treated as lower priority compared to large, high-revenue customers for order acceptance and scheduling. In the worst case, there may not be enough assessment capacities available for individual product categories by the deadline. Technically compliant products might then be prevented from being marketed on time solely due to a lack of testing capacities. This would delay market access, distort competition, and restrict product availability.

Improvement Proposal

The European Commission and national accreditation bodies should prioritize the designation of notified bodies and transparently report on available and planned capacities. If bottlenecks emerge, temporary and legally secure transition solutions must be implemented early. For this, as long as they are equivalent, existing product-specific certifications and evidence, as well as suitable conformity assessment bodies from selected third countries, should be recognized. In addition, during the transition phase described in Scenario 12, the manufacturer's self-declaration according to Module A should remain possible.

Scenario 15: Lack of Risk-oriented Enforcement in the CRA Rollout Phase

Starting Point

Achieving full CRA compliance requires not only technical adjustments in many companies. Documented, traceable, and auditable development, vulnerability management, and compliance processes must be established and integrated into existing workflows. The starting level, maturity, and product portfolio vary significantly, especially among small and medium-sized enterprises.

CRA Challenge

Depending on the size of the company and the product portfolio, this transformation can take several years. Companies need to address technical and organizational deficiencies simultaneously, even though central design aids and evidence bases are partially unavailable. As a result, at the start of the applicability, there may still be formal or procedural gaps in products without a concrete security issue. Enforcing all requirements indiscriminately from day one would treat actual product risks and mere evidence deficiencies equally.

Possible Consequence

Small and medium-sized manufacturers might be forced to temporarily withdraw products from the market or halt their development, even though there is no specific additional cybersecurity risk posed by them. Manufacturers, traders, and users would face significant legal uncertainty, while necessary process and product adaptations cannot be quickly implemented. This could trigger market exits, supply bottlenecks, and strains on existing digital value chains.

Improvement Proposal

During the initial phase of CRA application, market surveillance should proceed in a risk-oriented and proportional manner. In cases of formal or procedural deficiencies without a concrete security risk, companies should first be granted a reasonable period to rectify them. Immediate sales restrictions and other drastic measures should primarily focus on cases where a product poses an actual cybersecurity risk.

Cross-sectional Requirement: Risk-based Interpretation of Annex I

Products with digital elements vary significantly in terms of architecture, deployment environment, threat model, and update possibilities. Individual requirements of Annex I can therefore have different impacts on the actual security level depending on the context. This includes the assessment of vulnerability exploitability and update channels, which, in particularly isolated systems, can create additional attack surfaces. In the absence of clear assessment standards, manufacturers, conformity assessment bodies, and market surveillance authorities can reach different conclusions. A purely formal application can, in individual cases, favor technically inappropriate measures or impair proven security architectures.

Therefore, the requirements of Annex I should be consistently interpreted based on risk and considering the specific context of use. The European Commission and ENISA should develop practical guidelines with criteria, threat models, and relevant borderline cases. Alternative technical measures should be possible if an equivalent security level can be demonstrably achieved.

Conclusion

The goals pursued with the CRA are expressly supported by the industry. However, the outlined scenarios reveal recurring structural challenges. These stem less from a lack of willingness to implement and more from regulatory requirements that do not adequately consider technical dependencies, complex supply chains, different product life cycles, limited evaluation capacities, and the diversity of covered products.

This results in legal uncertainty, disproportionate evidence efforts, and practical implementation problems. Even manufacturers with a high security level can struggle to demonstrate compliance on time if relevant standards, guidelines, supplier information, or evaluation capacities are not available in a timely manner. At the same time, there is a risk that safe products are removed from the market, necessary updates or adjustments are delayed, and specialized providers face structural disadvantages. This can weaken competition, product availability, and the resilience of European supply chains.

Therefore, the CRA should be implemented more risk-based, proportionally, and along the product life cycle. Clear interpretation aids, practical evidence procedures, recognition of existing certifications and test reports, and appropriate transitional arrangements are needed when conditions for conformity assessment are lacking. It is crucial that the regulatory implementation addresses actual security risks and gives companies the leeway to adopt suitable technical and organizational measures in different products and environments.