Cyber Resilience Act

An updated position paper on the transposition at the European Level

February 2026

bitkom

At a glance

Cyber Resilience Act

The ongoing digital transformation increases exposure to cyber threats, while many products and services still fail to follow «security by design and by default" and do not ensure security across their full life cycle. Against this backdrop, EU regulation that sets a binding minimum level of cybersecurity is essential to protect states, businesses, and citizens while strengthening the competitiveness and strategic position of the European Economic Area.

Horizontal frameworks such as the Cyber Resilience Act create uniform EU-wide standards, prevent a harmful 'race to the bottom' and form a key foundation for Europe's digital economy. This paper therefore sets out concrete proposals to further improve the CRA, with the aim of keeping requirements clear, proportionate, and workable in practice while maintaining strong security outcomes across the Single Market.

Important takeaways

Bitkom proposes numerous compromise lines for a practicable CRA. The following three takeaways highlight a selection of these recommendations:

- **Align CRA with sector rules and global standards**

  Avoid duplicate testing by recognising evidence from vertical legislation and trusted international standards; accept equivalent third-country conformity bodies until EU standards/notified bodies are available.

- **Set realistic timelines and transitional rules**

  Link obligations (incl. vulnerability reporting) to 11 December 2027, publish standards early, and allow a two-year transition with self-declaration (Module A) if harmonised standards miss the 11 December 2026 milestone; use common specifications temporarily.

- **Enable pragmatic treatment of legacy products**

  Prevent market disruption by deeming products first placed on the market before 11 December 2027 compliant via flexible modules (e.g., Annex VIII Module H), with a risk-based approach for low-risk products.

Bitkom number

34 percent

of German companies registered a ransomware attack in 2025; three years before, this figure was only 12 percent (according to a study by Bitkom Research).

59%

of German companies consider cyber attacks to be a threat to their existence (according to a study by Bitkom Research).

Content

Cyber Resilience Act

An update position on the transposition at EU level

The ongoing digital transformation increases the vulnerability to cyber threats. Key products and services are often not designed according to the principle of «security by design and by default" and do not guarantee security throughout their life cycle. Against this backdrop, European regulation to establish a binding minimum level of cybersecurity is essential. It protects states, companies, and citizens, strengthens the competitiveness of the European Economic Area, and creates a strategic advantage in global competition.

Strong cybersecurity builds trust among customers and business partners and minimizes the risk of costly production downtime, liability claims, operational failures, harms to health or safety, and data leaks. Holistic cybersecurity protects both users, supply chains and critical IT infrastructures. Horizontal regulations such as the Cyber Resilience Act (CRA) establish uniform security standards across the EU. This ensures a minimum level of cybersecurity for all market participants and prevents a «race to the bottom" that is harmful to customers, businesses, and society.

Cybersecurity regulations such as the CRA are therefore a fundamental building block for a digital economy in Europe. Although we recognize the fundamentally positive development, we see, as outlined below, that there is still potential for optimization in the CRA.

Efficient interaction with sector-specific regulations and standards

With horizontal regulations such as CSA, CRA, DORA and NIS-2, the regulatory environment for cybersecurity in the EU has expanded significantly. In addition, vertical, sector-specific regulations – such as the Radio Equipment Directive (EU) 2014/53, the new Machinery Regulation (EU) 2023/1230, civil aviation (EU) 2018/1139 and the automotive industry (EU) 2019/2144 already regulate the cybersecurity and certification of certain systems and components.

The implementation of the CRA must not create duplicate structures or overlap with existing, recognised testing procedures. Duplicating testing and verification efforts causes high costs and avoidable bureaucracy without bringing any additional benefits. Duplicate structures place a disproportionate burden on small and medium-sized enterprises in particular.

Solution: The complexity of the regulations and the scope of mandatory safety certifications within the CRA should be limited to what is necessary and reasonable. Evidence already provided to demonstrate compliance with vertical requirements and technical specifications must be recognised in order to avoid duplicate testing and

assessments. International industry standards such as EMVCo or GSMA offer a comparable level of safety that is recognised throughout Europe and should therefore be explicitly taken into account, as their use prevents unnecessary extra work and strengthens competitiveness. In addition, comparable conformity assessment bodies from selected third countries, such as the UK, Japan and Australia, should be recognised, particularly while harmonised European standards and notified bodies are unavailable. This facilitates practical implementation, prevents bottlenecks in testing capacities and accelerates market access for secure products.

Coordinated interaction between existing sectoral regulations, international standards and CRA requirements is therefore crucial for practical implementation. Making targeted use of synergies and avoiding parallel structures and inconsistencies will ensure that the CRA increases the level of security in the European single market without hampering innovation and competitiveness. Bitkom therefore calls for consistent, globally compatible and low-bureaucracy implementation that keeps companies capable of acting and strengthens Europe's digital security.

Practicable deadlines for standardisation and implementation

The successful implementation of the CRA depends largely on downstream measures, in particular the publication of delegated acts and the development and listing of harmonised standards. Until these steps are completed, the industry is already taking extensive measures to ensure the highest possible level of CRA compliance. To this end, companies are drawing on established industry best practices, such as those relating to the handling of vulnerabilities. It is expected that future standards will adopt these approaches and not deviate from them fundamentally. The aim is to significantly reduce the subsequent adjustment effort and avoid short-term, resource-intensive changes. At the same time, organisational issues relating to internal processes, such as the systematic assessment of dependencies in the event of vulnerabilities in shared internal libraries, can already be addressed today.

Nevertheless, there remains a considerable dependence on downstream measures. In particular, the timing of the development and listing of harmonised standards is currently causing considerable planning uncertainty for manufacturers, distributors and importers.

The standards for dealing with vulnerabilities are to be made available to manufacturers by 30 August 2026, just a few days before the reporting requirements for actively exploited vulnerabilities and serious incidents come into force on 11 September 2026. Although this standard is being developed with Annex I of the CRA in mind, most of the content of the standard is required to be able to fulfil reporting obligations with respect to Art. 14.

The publication of further standards is also planned shortly before the relevant deadlines, provided that the ambitious plans are adhered to. Further product-specific Type C (vertical) standards on 30 October 2026. This would leave about a year for the implementation of product-specific standards, which is already very tight. Further horizontal Type B standards have been announced for 30 October 2027, about one and

a half months before the CRA comes into force. This leaves manufacturers little to no time to adapt their security measures and processes to the harmonised standards.

Given these timelines, it is clear that manufacturers and notified bodies face significant challenges in bringing all products to market in compliance with CRA requirements by 11 December 2027. This applies to both standard category products, which are subject to horizontal standards and account for the majority of products under CRA, and important and critical products. Manufacturers of all of these products are at risk of heavy penalties or loss of market access.

Solution: The European Commission should set realistic, reliable and technically feasible deadlines. The implementation of the CRA in companies must follow the standards, guidelines and secondary legislation – not pre-empt them. In many cases, the current timetables cannot be met and therefore need to be adjusted promptly in order to create planning security.

To ensure the safe and responsible handling of vulnerabilities, the start of reporting obligations should be linked to the date of general applicability of the CRA on 11 December 2027. The European Commission should also recognise existing and proven standards for reporting procedures. This would give companies and authorities alike planning security and avoid unnecessary duplication of structures.

In order to avoid bottlenecks in the availability of CRA-compliant products and components, we propose the possibility of a transitional arrangement. If, on 11 December 2026 – one year before the CRA comes into full effect – it is no longer possible to list the harmonised standards using the regular procedure, a two-year transitional period should apply. This transitional period should be between the publication of the relevant harmonised standards in the Official Journal of the EU (OJEU) and the first obligation to comply with the requirements. During such a transitional period, Class I and II products, as well as products in the standard category, should continue to have the option of manufacturer self-declaration in accordance with Module A.

In addition, the European Commission should avoid increasing reliance on common specifications in place of harmonised standards. Such a change would undermine the fundamental principles of the European standardisation system – openness, transparency and consensus – and carries the risk of reduced stakeholder participation and market fragmentation. Common specifications are often not internationally harmonised, which creates barriers for European companies and may lead to divergent policy approaches abroad. Common specifications should only be used as an explicitly temporary transitional solution.

Placing legacy products on the market after the transition period

The CRA expands the meaning of the CE mark to include the dimension of ‘cybersecurity’ for the first time and makes cybersecurity a mandatory property of digital products. At the same time, the CRA currently lacks a practical approach for existing product portfolios that were developed and first placed on the market before 11 December 2027. After the transition periods have expired, these products will also

be fully subject to the CRA requirements when they are placed on the market again, regardless of whether they have been substantially modified. Given the thousands of existing hardware and software products, a complete redevelopment within 30 months is not realistically feasible.

If the current definition of 'placing on the market' under the CRA and Blue Guide remains unchanged, there is a risk of significant market disruption. Numerous proven products could no longer be offered after the cut-off date. As a result, product discontinuations, temporary interruptions in the value chain of the EU internal market, and the withdrawal of companies or fundamental changes to their business models are to be expected. Such consequences may also affect products that pose a negligible risk to cybersecurity. This would weaken innovation, the competitiveness of smaller manufactures and overall jeopardise the supply of established digital solutions to users.

Solution: The issue of 'old products' must not become a structural problem for European value chains, particularly if there are no adequate alternatives. Together with the European Commission and the European standardisation organisations CEN, CENELEC and ETSI, a pragmatic approach to conformity for existing products should be developed to avoid far-reaching bans. A solution for existing products can be achieved through appropriate conformity assessment modules, such as Annex VIII Module H of the CRA.

In addition, a balanced and risk-based approach is needed for 'harmless' products. This will enable the CRA's objectives to be achieved effectively without placing an unnecessary burden on Europe's digital economy.

Simplification of reporting and documentation requirements

Article 14 of the CRA obliges manufacturers to report actively exploited vulnerabilities and severe security incidents via a specific platform in three steps: an early warning to the CSIRT and ENISA within 24 hours, a detailed report within 72 hours, and a final report within 14 days of the corrective measures being implemented. This system duplicates existing GDPR, DORA and NIS-2 frameworks and diverts resources away from the actual remediation.

Solution: To improve efficiency, the reporting procedure should be streamlined to two steps: an initial report within 72 hours with the essential information and a comprehensive report within 14 days after the corrective action. All reports should be submitted only once at EU-level, ideally via the ENISA platform, to avoid parallel processes. In addition, we advocate making the simplified documentation requirements for SMEs applicable to all manufacturers.

To avoid duplicate reporting processes, the reporting requirements under CRA, NIS-2, DORA and GDPR should be fully harmonised. A single report to a competent authority – ideally via a central ENISA platform – should fulfil all parallel reporting obligations ('once-only'). This will focus resources on remediation and risk reduction and avoid unnecessary redundancies. All EU member states' reporting authorities should be able to communicate in English to avoid misunderstandings and inconsistencies, especially

when manufacturers report centrally from their EU headquarters where cybersecurity experts may not speak all official EU languages.

Switching between cloud services

The distinction between 'products with digital elements' and pure cloud services is increasingly fluid, as functionally identical services are often provided through a mix of cloud processing and local software components. This technical fluidity, however, is met with a rigid regulatory binary that creates significant legal uncertainty. In practice, a cloud service governed by the NIS-2 Directive can abruptly shift into the scope of the CRA as soon as even a minor software component—such as a local agent or client—is delivered to the customer for local installation. This transition is inherently problematic because the requirements of NIS-2 and the CRA are not harmonized, leading to inconsistent and often conflicting compliance paths for the same service ecosystem. Furthermore, once a product falls within the CRA's reach, it must immediately demonstrate CE marking according to the NLF. This creates a severe structural break, as the NLF's traditional, product-centric logic offers no flexibility for the agile, service-oriented nature of the modern software and cloud sector.

Solution: One potential path could be the introduction of a de minimis or materiality threshold under the CRA, allowing products with only negligible amounts of distributed software compared to their overall cloud-based functionality to be exempted from its requirements, based on the proportion of total code involved. Another solution could be a presumption of conformity between NIS-2 and the CRA, possibly facilitated through the European Cybersecurity Certification Framework (ECCF). This would allow for a more seamless integration of requirements without imposing redundant bureaucratic hurdles. Furthermore, a clarifying interpretation of the system of placing products on the market could be helpful. Neither a change in the distribution channel nor provision via the cloud should be considered a new placing on the market; clear guidelines must be provided for this.

Standardisation and classification of hybrid security products (EDR/XDR)

EDR and XDR solutions typically combine functions that lie between Class I products such as anti-malware and Class II products such as firewalls, intrusion detection or intrusion prevention systems. There is currently no clear classification. A blanket reference to 'core functions' is insufficient because adding or omitting individual functional modules changes the risk profile and thus the product character.

Solution: Hybrid products require a reliable framework that reflects classification and the choice of standards in a practical manner. Bitkom recommends that the presumption of conformity be designed in such a way that manufacturers can alternatively choose a relevant harmonised standard or demonstrate the combination of several relevant standards. In addition, regulatory and technical guidelines should be provided that address the classification of hybrid products and the handling of functional changes, including clear thresholds for 'significant changes'.

Standardisation and implementation deadlines should be set in such a way that complex security products remain certifiable in a predictable manner.

Digital supply chains and dependencies

A clear picture of suppliers and available technological resources is essential for assessing a company's security. This allows risks between companies and their critical suppliers to be evaluated. However, modern software development relies heavily on external libraries and components, often in the form of open-source software. Taking transitive dependencies into account, thousands of components can flow into a single product. In practice, there are two key limitations: Firstly, dependencies cannot always be fully identified because there are no completely effective methods available for doing so. Secondly, manual individual testing is not feasible given the number of components involved. In view of these limitations, the introduction of Open Source Software Stewards by the CRA does not represent a complete solution, and considerable uncertainty remains.

Solution: Ideally, automated solutions based on modular architectures could be used, enabling immediate feedback on relevant authorisations for individual components. In conjunction with advanced development tools, modern architectures also allow a Software Bill of Materials (SBOM) to be generated consistently across the entire supply chain. However, such solutions are not yet widely available in the required quality and cost-effectiveness. Against this background, manufacturer obligations should be limited to what is actually feasible to ensure that small and medium-sized enterprises can also meet the requirements. Bitkom therefore recommends the use of established supply chain risk management (SCRM) models that enable a transparent representation of the risk situation of components and assign responsibilities in a practical manner. International standards, such as ISO 31000, should serve as a reference framework for the design of SCRM models. Any additional costs beyond this basic model should remain voluntary or be focused on a small number of particularly critical libraries and products.

Seamless transition from RED-DA to CRA compliance

In order to avoid double regulation of products that fall under both the Radio Equipment Directive RED-DA (EU) 2022/30 and the CRA with regard to cybersecurity, the RED-DA is to be repealed in good time for the CRA to become applicable. However, this will involve a very short transition period of only six months to demonstrate CRA compliance for all RED-DA products from 11 December 2027 onwards (see Art. 69.1 CRA).

Solution: In order to avoid unnecessary multiple testing of digital products for RED-DA and CRA between 2026 and 2028 and to enable as seamless a transition as possible from RED-DA to CRA compliance, it would make sense to consider all products that are (prematurely and voluntarily) CRA-compliant as also compliant with RED-DA.

An alternative approach would be to extend the transition period under Article 69.1 from 6 months to 12 months until December 31, 2028.

Improvements to cybersecurity do not constitute a ‘significant change’

The regulations on ‘significant changes’ in the CRA pose considerable challenges for manufacturers. The underlying concept originates from the EU's NLF and is only applicable to digital products to a limited extent. It follows a strongly product-centric control logic that is incompatible with the realities of modern software development. In practice, development and security processes must be evaluated, not individual software versions – with a few exceptions, such as software for space applications, where long certification cycles are justifiable. The current definition of a significant change is too broad for software. It also covers regular adjustments that are common in agile development, leading to renewed conformity assessments for everyday updates. This is disproportionate to the actual risk.

The example of an agile standard product such as a browser shows that a brief risk assessment is often sufficient and regularly leads to a reduction in risk. However, classifying such changes as significant would require comprehensive formal steps – from updating the technical documentation to a new declaration of conformity and possible external audits. This can lead to security-enhancing measures being delayed or not implemented for economic reasons, even though they would increase the level of cybersecurity.

Solution: The Commission should provide clear and practical guidelines with thresholds and examples to ensure legal certainty in determining significant changes. In particular, security updates and security enhancements that close security gaps, enhance cybersecurity protection, or further reduce security risks should not constitute a ‘significant change’ within the scope of the CRA.

The definition of a substantial change must therefore take particular account of the specific characteristics of modern software development and define these much more narrowly. In our opinion, the definition of a substantial change should be limited to changes to the core function.

Uniform framework conditions for market surveillance and customs in the EU

Manufacturers are confronted with an extremely fragmented supervisory environment in which, among other things, more than 27 different market surveillance authorities can submit requests in an uncoordinated manner. In addition to the CRA, the complex EU cybersecurity legislation, which includes NIS-2, CSA, DORA, RED-DA and the AI Act, can also lead to different national interpretations and implementations. As a result, manufacturers are faced with a kind of ‘location lottery’ within the EU, because the inconsistent resources, staffing, and competences of market surveillance and custom

authorities can lead to inconsistent assessments and enforcement of CRA requirements.

Solution: To avoid unequal treatment, a harmonised approach is urgently needed. The lead market surveillance authority, which acts as the central coordination point for regulatory enquiries, should be designated based on the location of a manufacturer's main establishment in the EU.

The EU Commission should also develop common interpretation guidelines and provide standardised implementation frameworks including minimum staffing requirements. In addition, the necessary resource and competence development should be actively promoted in a uniform manner across the EU, for example through ENISA or through coordinated national efforts that provide uniform training and tools. Finally, regular peer reviews of national monitoring structures and results would ensure the most consistent enforcement possible and thus ensure a level playing field for all market participants across the EU.

In addition to the designation of a lead authority, risk-based plausibility screenings are necessary. Market surveillance and custom authorities should automatically check the (possibly reduced) technical documentation for plausibility and anomalies and use this as a trigger for in-depth checks. This requires uniform tools, common interpretation guidelines, EU-wide resource and competence building, similar staffing requirements, and regular peer reviews to ensure consistent enforcement and a level playing field.

Consistent CRA enforcement for EU imports

The CRA's highly ambitious implementation targets and considerable bureaucratic requirements are creating structural competitive disadvantages for European software providers: delays in time-to-market and restrictions on the availability of compliant products are hampering innovation and are at odds with current political initiatives to strengthen the EU's competitiveness, such as those under the Omnibus package.

The fundamental flaw in the current approach lies in the failure to sufficiently distinguish between physical hardware products and pure software. This is clearly illustrated by the example of software products that can be marketed without physical delivery. Unlike a refrigerator or a mechanical component, software is often accessed, downloaded, or used via global web shops and repositories. Downloads from stores outside the European Union can only be prevented to a limited extent; even physical deliveries are difficult to control completely in practice. Non-European providers, on the other hand, can often effectively evade CRA enforcement. In the private customer segment, this carries the risk of a shadow economy and, in the industrial sector, creates considerable implementation risks for integrators who install components in their end products. As reported by stakeholders in specialized sectors like aerospace, third-country providers with a monopoly position may simply refuse to comply with CRA standards. If non-European suppliers fail to provide evidence or refuse to cooperate in ensuring compliance, European manufacturers find themselves in a situation where they are expected to guarantee the safety of components over which they have no control and no legal leverage.

Solution: To deal with these situations, the CRA must move beyond its approach modelled on hardware regulation. Political and regulatory cooperation instruments are needed that enable enforcement against non-European manufacturers and, where appropriate, draw on internationally recognised standards and conformity assessment bodies. Suitable solutions can already be found in other areas of EU product regulation, where the enforcement problem vis-à-vis third-country suppliers is addressed by always clearly naming an economically responsible actor based in the EU (e.g. manufacturer, importer, authorised representative or fulfilment service provider) must always be clearly named and products without sufficient evidence may not be legally placed on the market. The lack of cooperation from non-European suppliers cannot simply be compensated for by market access barriers, as this would force the replacement of critical components where no viable alternatives exist.. Instead, official guidance is needed that describes how to deal with uncooperative suppliers, including scenarios in which it is not possible to terminate the business relationship. In such cases, manufacturer obligations must be strictly limited to what is actually feasible in the digital reality to avoid disproportionate burdens and competitive disadvantages.

Limited deadlines for reporting vulnerabilities in existing products

The CRA also introduces indefinite obligations to report vulnerabilities and incidents. Unlike vulnerability management obligations, which end when support expires, these reporting obligations currently apply without restriction. Such indefinite obligations are disproportionate. In addition, this indefinite reporting obligations apply not only to all upcoming CRA-relevant products but also to all legacy products with digital elements that were placed on the market before the CRA came into force and therefore puts longstanding EU-based manufacturers at an additional disadvantage.

Solution: Monitoring and reporting obligations should be limited to a specific period or reduced to the end of support.

Joint conformity assessment with the AI Regulation

The increasing complexity resulting from parallel conformity assessments under the CRA and the AI Act leads to considerable additional work. A lack of coordination between the procedures encourages inconsistencies, duplication of effort and makes it difficult to implement both pieces of legislation in a coherent manner. In particular, different assessment structures and responsibilities increase the administrative burden on companies and conformity assessment bodies.

Solution: The conformity assessments of the CRA and the AI Act should be better coordinated. Common procedures and mutual recognition of assessments can avoid duplication of work and promote consistency. This could be achieved through a common conformity assessment framework that integrates CRA modules B, C and H (in accordance with Decision 768/2008/EC) with the internal (Annex VI) and external assessments (Annex VII) of the AI Act. In addition, conformity assessment bodies with

overlapping competences should be authorised to assess conformity under both legal acts, and mutual recognition agreements should stipulate that compliance with one framework (e.g. Annex VII of the AI Act) is equivalent to compliance with the equivalent CRA requirements.

Rules and conditions for affixing the CE marking

Another challenge in implementing the CRA is the full introduction of CE marking for basic electronic components (such as semiconductors). Such components are intended exclusively for integration into other products and do not fulfil any specific application on their own. In the context of the supply chain, packaging labels are already widely used for traceability and to verify compliance with normative requirements by integrators. An additional CE marking directly on the individual components is neither reliably visible nor does it offer any additional enforcement depth compared to the creation of technical documentation and the associated declaration of conformity for these components, given size and legibility limitations and the influence of assembly and environmental factors (such as reflow soldering, overmoulding or the application of coatings).

Solution: In order to ensure uniform treatment of this issue and regulatory proportionality in the European market, the ECR should be extended to include a specific exemption for such products from the CE marking requirement, analogous to the Machinery Directive ('incomplete machinery').

Exemption for 'products that are inherently safe'

Finally, the scope of the CRA also extends to millions of extremely trivial products such as A/D converters, USB charging devices, or trivial semiconductor components such as memory chips or logic gates. Although these products pose virtually no cybersecurity risk, they are still subject to full conformity assessment under the new legal framework, including extensive testing, labelling and documentation requirements.

Solution: As specified in the Machinery Directive ('non-hazardous machinery') and the EMC Directive ('inherently safe products'), a specific exemption for 'inherently safe products' should be included in the CRA. This category would apply to products with digital elements that cannot pose cybersecurity risks due to their technical simplicity.

Relieving bureaucracy for SMEs

The process of conformity assessment according to CRA specifications is very complex: a risk assessment must be carried out and documented, safety specifications derived from it and tested. Extensive technical documentation must be created. Among other things, this must be kept up to date after significant changes. In addition, reported vulnerabilities must be mentioned in it. Conformity assessments must be carried out and declarations of conformity completed. For the vast majority of SMEs, but also for

larger companies, this process is not both legally compliant and economically feasible due to the effort involved.

Solution: Essentially, the majority of the documentation requirements need to be eliminated. SMEs in particular should be able to establish a presumption of conformity with CRA requirements by committing to high cybersecurity standards and providing a plausible description of their own processes. This commitment can be reviewed by market surveillance authorities if there is reasonable suspicion of non-compliance. Products listed in Annex IV could be exempted from this procedure.

CRA Blue Guide: Conformity assessment according to Module H

The CRA Blue Guide describes conformity assessment in accordance with Module H and cites an ISO 9001 QMS as an example, taking CRA requirements into account – we welcome this. However, the requirement that the inclusion of a new product or any 'significant change' triggers a reassessment of the QMS by a conformity assessment body is problematic. This is not practical for software due to agile development cycles: the broad definition of significant changes (e.g. change of authentication method) would require regular external audits for frequent releases. This particularly affects cybersecurity products, which require ongoing security updates due to changing threats; functional updates are also standard. Such a recertification requirement defeats the purpose of a QMS. Signature updates can also give rise to new risks (see CrowdStrike outage in 2024), which is why fast, internally automated testing – i.e. an effective QMS – is crucial.

Solution: For a legally compliant and practical process, the recertification requirements should comply with ISO 9001: A QMS according to Module H must cover new and significantly modified products without event-related external assessment. With a correspondingly broad QMS scope, regular audits (annual, recertification after three years) are sufficient. An external audit should only be required for the initial manufacture of a product in a new class according to Annex III/IV CRA.

Bitkom represents more than 2,300 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Felix Kuhlenkamp | Head of Security
T +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Responsible Bitkom Committee
WG Security Policy