Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Comments

EU-Cyber Resilience Act

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:

Berlin, 24 March 2025

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV),
for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de
www.german-banking-industry.org

Comments EU-Cyber Resilience Act

The German Banking Industry Committee fully recognizes that the Cyber Resilience Act will enhance cybersecurity standards of products that contain a digital component, requiring manufacturers and retailers to ensure cybersecurity throughout the lifecycle of their products from 2027 onward.

Therefore, we welcome rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products using essential cybersecurity requirements for the design, development and production of products with digital elements, and by establishing obligations for economic operators in relation to those products with respect to foster cybersecurity.

The scope of the Cyber Resilience Act applies to all products connected directly or indirectly to another device or network except for specified exclusions such as certain open-source software or services products that are already covered by existing rules.

This means that the Cyber Resilience Act as horizontal product-regulation rightfully recognizes that it co-exists in a broader landscape of cybersecurity policies and that cybersecurity may already be regulated by sector-based policies or product-specific rules, e.g. by NIS 2 or by the Digital Operational Resilience Act (DORA) as lex specialis to NIS 2.

Today the Cyber Resilience Act contains five explicit exemptions in Article 2 (2) to 2 (4). Those exemptions apply today to products with digital elements that are subject to specific legal acts (e.g. for medical devices) or to certified products.

To ensure that the CRA remains future-proof and does not create additional bureaucratic burden, Article 2 (5) also contains an opening clause that would allow for a limitation or an exclusion for products "covered by other Union rules laying down requirements that address all or some of the risks covered by the essential cybersecurity requirements set out in Annex I" when (i) such limitation or exclusion is consistent with the overall regulatory framework that applies to those products; and (ii) the sectoral rules achieve the same or a higher level of protection as that provided for by this Regulation.

We are of the opinion that EU-wide by Financial Sector distributed digitalized financial products (e.g. mobile payment applications, payment cards, banking apps for servicing payment accounts, Automated Teller Machines for making cash disbursements and Point-of-Sale-terminals for accepting card payments) are eligible for such a limitation or exclusion given in Article 2 (5).

This paper outlines how the Digital Operational Resilience Act (DORA) as the overarching framework for the Financial Sector fulfils the requirement of the opening clause and would qualify for a respective Delegated Act by the European Commission.

o Even though DORA is not product-specific regulation, it requires financial institutions to establish an end-to-end framework for Information and Communication Technology (ICT) systems and assets.

Comments EU-Cyber Resilience Act

o Applicable requirements cover the whole lifecycle of those ICT systems, from development, to implementation, ongoing application/ use and decommissioning. Throughout the whole lifecycle, DORA mandates – in a risk-based manner – documentation, monitoring, Vulnerability and patch management, incident identification, handling and reporting, as well as testing. Also, it sets more broadly requirements around the governance of ICT risk management and strategy.

o Despite the fact that DORA is not product-specific, the customer focus is addressed, too and is equally protected by DORA. DORA's overarching perspective goes way beyond the process of bringing a new product to market, as internal processes and systems are strictly scrutinized by supervisors to reduce and mitigate risks for the financial institution, customer assets and financial stability. Communication strategies for incidents are an integral part of the framework overall and create awaren ess with customers as appropriate and necessary.

Comments EU-Cyber Resilience Act

CRA Requirement	*DORA*
ANNEX I **ESSENTIAL CYBERSECURITY REQUIREMENTS** Part I Cybersecurity requirements relating to the properties of products with digital elements (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.	*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_16* *Art. 16 subparagraph 1 and 2 RTS Risk Management:* 1. As part of the safeguards to preserve the availability, authenticity, integrity, and confidentiality of data, financial entities shall develop, document and implement a policy governing the acquisition, development, and maintenance of ICT systems. That policy shall: […] 2. Financial entities shall develop, document, and implement an ICT systems' acquisition, development, and maintenance procedure for the testing and approval of all ICT systems prior to their use and after maintenance, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). The level of testing shall be commensurate to the criticality of the business procedures and ICT assets concerned. The testing shall be designed to verify that new ICT systems are adequate to perform as intended, including the quality of the software developed internally. […] 3. […] - 9. […]
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (a) be made available on the market without known exploitable vulnerabilities;	*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_10* *Art. 10 subparagraph 2 RTS Risk Management:* 2. The vulnerability management procedures referred to in paragraph 1 shall […] (d) track the usage of: (i) third-party libraries, including open-source libraries, used by ICT services supporting critical or important functions; (ii) ICT services developed by the financial entity itself or specifically customised or developed for the financial entity by an ICT third-party service provider; *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_16* *Art. 16 subparagraph 3 and 8 RTS Risk Management:* 3. The procedure referred to in paragraph 2 shall contain the performance of source code reviews covering both static and dynamic testing. That testing shall contain security testing for internet-exposed systems and applications in accordance with Article 8(2), point (b), points (v), (vi) and (vii). Financial entities shall: (a) identify and analyse vulnerabilities and anomalies in the source code; (b) adopt an action plan to address those vulnerabilities and anomalies; (c) monitor the implementation of that action plan. […] 8. The procedure referred to in paragraph 2 shall provide that proprietary software and, where feasible, the source code provided by ICT third-party service providers or coming from open-source projects, are to be analysed and tested in accordance with paragraph 3 prior to their deployment in the production environment.
(2) On the basis of the cybersecurity risk	*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_8* *Art. 8 subparagraph 1 and 2 RTS Risk Management:*

Comments EU-Cyber Resilience Act

assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;	1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement policies and procedures to manage the ICT operations. Those policies and procedures shall specify how financial entities operate, monitor, control, and restore their ICT assets, including the documentation of ICT operations. 2. The policies and procedures for ICT operations referred to in paragraph 1 shall contain all of the following: (a) an ICT assets description, including all of the following: (i) requirements regarding secure installation, maintenance, configuration, and deinstallation of an ICT system; […] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_11* *Art. 11 subparagraph 1 and 2 RTS Risk Management:* 1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement a data and system security procedure. 2. The data and system security procedure referred to in paragraph 1 shall contain all of the following elements related to data and ICT system security, in accordance with the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554: (a) the access restrictions referred to in Article 21 of this Regulation, supporting the protection requirements for each level of classification; (b) the identification of a secure configuration baseline for ICT assets that minimise exposure of those ICT assets to cyber threats and measures to verify regularly that those baselines are effectively deployed; (c) the identification of security measures to ensure that only authorised software is installed in ICT systems and endpoint devices; […] For the purposes of point (b), the secure configuration baseline referred to in that point shall take into account leading practices and appropriate techniques laid down in the standards defined in Article 2, point (1), of Regulation (EU) No 1025/2012.
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_17* *Art. 17 subparagraph 3 DORA Regulation:* […] 3. The ICT-related incident management process referred to in paragraph 1 shall: […] (d) set out plans for communication to staff, external stakeholders and media in accordance with Article 14 and for notification to clients, for internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate; […]

Comments EU-Cyber Resilience Act

users, and the option to temporarily postpone them;	https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_19 *Art. 19 subparagraph 1 and 3 DORA:* 1. Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 in accordance with paragraph 4 of this Article. […] 3. Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident. In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_10* *Art. 10 subparagraph 2,3 and 4 RTS Risk Management:* 2. (f) prioritise the deployment of patches and other mitigation measures to address the vulnerabilities identified; 3. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document and implement patch management procedures. 4. The patch management procedures referred to in paragraph 3 shall: (a) to the extent possible identify and evaluate available software and hardware patches and updates using automated tools; b) identify emergency procedures for the patching and updating of ICT assets; d) set deadlines for the installation of software and hardware patches and updates and escalation procedures in case those deadlines cannot be met.
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_17* *Art. 17 subparagraph 3 DORA Regulation:* […] 3. The ICT-related incident management process referred to in paragraph 1 shall: […] (d) set out plans for communication to staff, external stakeholders and media in accordance with Article 14 and for notification to clients, for internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate; […] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_19 *Art. 19 subparagraph 1 and 3 DORA:* 1. Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 in accordance with paragraph 4

Comments EU-Cyber Resilience Act

	of this Article. […] 3. Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident. In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_20* *Art.20 subparagraph 1 RTS Risk Management:* 1. As part of their control of access management rights, financial entities shall develop, document, and implement identity management policies and procedures that ensure the unique identification and authentication of natural persons and systems accessing the financial entities' information to enable assignment of user access rights in accordance with Article 21. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_21* *Art. 21 RTS Risk Management:* As part of their control of access management rights, financial entities shall develop, document, and implement a policy that contains all of the following: […] d) a provision on restrictions of access to ICT assets, setting out controls and tools to prevent unauthorised access; […] (f) authentication methods, including all of the following: […]
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;	*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_6* *Art. 6 subparagraph 2 RTS Risk Management:* Financial entities shall design the policy on encryption and cryptographic controls referred to in paragraph 1 on the basis of the results of an approved data classification and ICT risk assessment. That policy shall contain rules for all of the following: (a) the encryption of data at rest and in transit; […]
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_17* *Art. 17 subparagraph 3 DORA Regulation:* […] 3. The ICT-related incident management process referred to in paragraph 1 shall: […] (d) set out plans for communication to staff, external stakeholders and media in accordance with Article 14 and for notification to clients, for internal escalation

Comments EU-Cyber Resilience Act

by the user, and report on corruptions;	procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate; […] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_19 *Art. 19 subparagraph 1 and 3 DORA*: 1. Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 in accordance with paragraph 4 of this Article. […] 3. Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident. In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_6* *Art. 6 subparagraph 2 RTS Risk Management:* 2. Financial entities shall design the policy on encryption and cryptographic controls referred to in paragraph 1 on the basis of the results of an approved data classification and ICT risk assessment. That policy shall contain rules for all of the following: (a) the encryption of data at rest and in transit; (b) the encryption of data in use, where necessary; (c) the encryption of internal network connections and (d) the cryptographic key management referred to in Article 7, laying down rules on the correct use, protection, and lifecycle of cryptographic keys. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_16* *Art. 16 subparagraph 1 (c) RTS Risk Management:* 1. As part of the safeguards to preserve the availability, authenticity, integrity, and confidentiality of data, financial entities shall develop, document and implement a policy governing the acquisition, development, and maintenance of ICT systems. That policy shall: […] (c) specify measures to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during the development, maintenance, and deployment of those ICT systems in the production environment.
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements	*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#rct_26* *Recital (26) RTS Risk Management:* (26) The requirements for financial entities that are subject to the simplified ICT

Comments EU-Cyber Resilience Act

shall: (g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);	risk management framework referred to in Article 16 of Regulation (EU) 2022/2554 should be focused on those essential areas and elements that, in light of the scale, risk, size, and complexity of those financial entities, are as a minimum necessary to ensure the confidentiality, integrity, availability, and authenticity of the data and services of those financial entities. In that context, those financial entities should have in place an internal governance and control framework with clear responsibilities to enable an effective and sound risk management framework. Furthermore, to reduce the administrative and operational burden, those financial entities should develop and document only one policy, that is an information security policy, that specifies the high-level principles and rules necessary to protect the confidentiality, integrity, availability, and authenticity of data and of the services of those financial entities. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#rct_30* *Recital (30) RTS Risk Management:* (30) To the extent to which processing of personal data is required to comply with the obligations set out in this Act, Regulations (EU) 2016/679 (9) and (EU) 2018/1725 (10) of the European Parliament and of the Council should fully apply. For instance, the data minimisation principle should be complied with where personal data are collected to ensure an appropriate incident detection. The European Data Protection Supervisor has also been consulted on the draft text of this Act. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_8* *Art. 8 subparagraph 1 DORA:* As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_29 *Art. 29 subparagraph 2 DORA:* 2. […] Where contractual arrangements on the use of ICT services supporting critical or important functions are concluded with an ICT third-party service provider established in a third country, financial entities shall, in addition to the considerations referred to in the second subparagraph, also consider the compliance with Union data protection rules and the effective enforcement of the law in that third country. […] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_30 *Art. 30 subparagraph 2 DORA:*

Comments EU-Cyber Resilience Act

	The contractual arrangements on the use of ICT services shall include at least the following elements: […] (d) provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements; *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_11* *Art. 11 subparagraph 2 RTS Risk Management:* The data and system security procedure referred to in paragraph 1 shall contain all of the following elements related to data and ICT system security, in accordance with the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554: […] (i) the identification and implementation of security measures to prevent data loss and leakage for systems and endpoint devices; […] (k) for ICT assets or services operated by an ICT third-party service provider, the identification and implementation of requirements to maintain digital operational resilience, in accordance with the results of the data classification and ICT risk assessment.
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_9* *Art. 9 subparagraph 4 DORA:* As part of the ICT risk management framework referred to in Article 6(1), financial entities shall: (a) develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable; *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_12* *Art. 12 subparagraph 2 DORA:* Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardise the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_13* *Art. 13 DORA:* […] 4. Financial entities shall monitor the effectiveness of the implementation of

Comments EU-Cyber Resilience Act

	their digital operational resilience strategy set out in Article 6(8). They shall map the evolution of ICT risk over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understanding the level of ICT risk exposure, in particular in relation to critical or important functions, and enhance the cyber maturity and preparedness of the financial entity. […] 7. Financial entities, […], shall monitor relevant technological developments on a continuous basis, also with a view to understanding the possible impact of the deployment of such new technologies on ICT security requirements and digital operational resilience. They shall keep up-to-date with the latest ICT risk management processes, in order to effectively combat current or new forms of cyber-attacks. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_17* *Art. 17 subparagraph 3 DORA* The ICT-related incident management process referred to in paragraph 1 shall: […] (f) establish ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_19* *Art. 19 subparagraph 3 DORA:* *3.*[…] In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_26* *Art. 26 subparagraph 2 DORA:* Each threat-led penetration test shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions. Financial entities shall identify all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those supporting the critical or important functions which have been outsourced or contracted to ICT third-party service providers. […] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_13* *Art. 13 subparagraph (f) RTS Risk Management:* Financial entities shall, as part of the safeguards ensuring the security of networks against intrusions and data misuse, develop, document, and implement policies, procedures, protocols, and tools on network security management, including all of the following: […] (f) the design of networks in line with the ICT security requirements established by the financial entity, taking into account leading practices to ensure the

Comments EU-Cyber Resilience Act

	confidentiality, integrity, and availability of the network;
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_9* *Art. 9 subparagraph 2 DORA:* Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_15* *Art. 15 DORA:* The ESAs shall, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards in order to: (a) specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 9(2), with a view to ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays; (b) develop further components of the controls of access management rights referred to in Article 9(4), point (c), and associated human resource policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risk through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices; […] *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_16* *Art. 16 subparagraph 1 DORA:* […] Without prejudice to the first subparagraph, the entities listed in the first subparagraph shall: […] (c) minimise the impact of ICT risk through the use of sound, resilient and updated ICT systems, protocols and tools which are appropriate to support the performance of their activities and the provision of services and adequately protect availability, authenticity, integrity and confidentiality of data in the network and information systems; […] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_2* *Art. 2 subparagraph 1 RTS Risk Management:* Financial entities shall ensure that their ICT security policies, information security, and related procedures, protocols, and tools as referred to in Article 9(2) of Regulation (EU) 2022/2554 are embedded in their ICT risk management framework. Financial entities shall establish the ICT security policies, procedures, protocols, and tools laid down in this Chapter that:

Comments EU-Cyber Resilience Act

	(a) ensure the security of networks; […] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_11* *Art. 11 subparagraph 2 RTS Risk Management:* The data and system security procedure referred to in paragraph 1 shall contain all of the following elements related to data and ICT system security, in accordance with the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554: […] (b) the identification of a secure configuration baseline for ICT assets that minimise exposure of those ICT assets to cyber threats and measures to verify regularly that those baselines are effectively deployed; (c) the identification of security measures to ensure that only authorised software is installed in ICT systems and endpoint devices; (d) the identification of security measures against malicious codes; (e) the identification of security measures to ensure that only authorised data storage media, systems, and endpoint devices are used to transfer and store data of the financial entity; […] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_13* *Art. 13 subparagraph (k) RTS Risk Management:* Financial entities shall, as part of the safeguards ensuring the security of networks against intrusions and data misuse, develop, document, and implement policies, procedures, protocols, and tools on network security management, including all of the following: […] (k) the implementation of a secure configuration baseline of all network components, and the hardening of the network and of network devices in line with any vendor instructions, where applicable standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012, and leading practices; […]
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (j) be designed, developed and produced to limit attack surfaces, including external interfaces;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_9* *Art. 9 subparagraph 4 DORA:* As part of the ICT risk management framework referred to in Article 6(1), financial entities shall: […] (c) implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof; *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_16* *Art. 16 subparagraph 1 (a) RTS Risk Management:* As part of the safeguards to preserve the availability, authenticity, integrity, and confidentiality of data, financial entities shall develop, document and implement a policy governing the acquisition, development, and maintenance of ICT systems. That policy shall:

Comments EU-Cyber Resilience Act

	(a) identify security practices and methodologies relating to the acquisition, development, and maintenance of ICT systems; […]
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401774#art_3* *Art. 3 DORA:* Financial entities shall develop, document, and implement ICT risk management policies and procedures that shall contain all of the following: […] (b) a procedure and a methodology to conduct the ICT risk assessment, identifying: (i) vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions; (ii) the quantitative or qualitative indicators to measure the impact and likelihood of the vulnerabilities and threats referred to in point (i); (c) the procedure to identify, implement, and document ICT risk treatment measures for the ICT risks identified and assessed, including the determination of ICT risk treatment measures necessary to bring ICT risk within the risk tolerance level referred to in point (a); (d) for the residual ICT risks that are still present following the implementation of the ICT risk treatment measures referred to in point (c): (i) provisions on the identification of those residual ICT risks; *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_9* *Art. 9 subparagraph 1 DORA:* 1. For the purposes of adequately protecting ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;	Same as Part I (2)(k)
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (m) provide the possibility for users to securely and	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_8 *Art. 8 RTS Risk Management:* 1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement policies and procedures to manage the ICT operations. Those policies and procedures shall specify how financial entities operate, monitor, control, and restore their ICT assets, including the

Comments EU-Cyber Resilience Act

easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	documentation of ICT operations. 2. The policies and procedures for ICT operations referred to in paragraph 1 shall contain all of the following: (a) an ICT assets description, including all of the following: (i) requirements regarding secure installation, maintenance, configuration, and deinstallation of an ICT system; (ii) requirements regarding the management of information assets used by ICT assets, including their processing and handling, both automated and manual; (iii) requirements regarding the identification and control of legacy ICT systems; (b) controls and monitoring of ICT systems, including all of the following: (i) backup and restore requirements of ICT systems; […] (c) error handling concerning ICT systems, including all of the following: (i) procedures and protocols for handling errors; (ii) support and escalation contacts, including external support contacts in case of unexpected operational or technical issues; (iii) ICT system restart, rollback, and recovery procedures for use in the event of ICT system disruption. For the purposes of point (b)(v), the separation shall consider all of the components of the environment, including accounts, data or connections, as required by Article 13, first subparagraph, point (a).
Part II Vulnerability handling requirements Manufacturers of products with digital elements shall: (1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_8* *Art. 8 subparagraph 2 DORA:* Financial entities shall, on a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401774#art_10* *Art. 10 RTS Risk Management, Vulnerability and patch management*
Part II Vulnerability handling requirements *Manufacturers of products with digital elements shall:* *(2)* *in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;*	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_7* *Art. 7 DORA:* *In* order to address and manage ICT risk, financial entities shall use and maintain updated ICT systems, protocols and tools that are: […] (b) reliable; […] (d) technologically resilient in order to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_9* *Art. 9 DORA:* […]

Comments EU-Cyber Resilience Act

	2. Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit. […] 4. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall: […] (e) implement documented policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner; (f) have appropriate and comprehensive documented policies for patches and updates. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_25* *Art. 25 subparagraph 1 and 2 DORA:* 1. The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing. 2. Central securities depositories and central counterparties shall perform vulnerability assessments before any deployment or redeployment of new or existing applications and infrastructure components, and ICT services supporting critical or important functions of the financial entity. […] *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401774#art_10* *Art. 10 RTS Risk Management:* 1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement vulnerability management procedures. 2. The vulnerability management procedures referred to in paragraph 1 shall: (a) identify and update relevant and trustworthy information resources to build and maintain awareness about vulnerabilities; (b) ensure the performance of automated vulnerability scanning and assessments on ICT assets, whereby the frequency and scope of those activities shall be commensurate to the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of the ICT asset; (c) verify whether: (i) ICT third-party service providers handle vulnerabilities related to the ICT services provided to the financial entity;

Comments EU-Cyber Resilience Act

	(ii) whether those service providers report to the financial entity at least the critical vulnerabilities and statistics and trends in a timely manner; (d) track the usage of: (i) third-party libraries, including open-source libraries, used by ICT services supporting critical or important functions; (ii) ICT services developed by the financial entity itself or specifically customised or developed for the financial entity by an ICT third-party service provider; (e) establish procedures for the responsible disclosure of vulnerabilities to clients, counterparties, and to the public; (f) prioritise the deployment of patches and other mitigation measures to address the vulnerabilities identified; (g) monitor and verify the remediation of vulnerabilities; (h) require the recording of any detected vulnerabilities affecting ICT systems and the monitoring of their resolution. For the purposes of point (b), financial entities shall perform the automated vulnerability scanning and assessments on ICT assets for the ICT assets supporting critical or important functions on at least a weekly basis. […] 4. The patch management procedures referred to in paragraph 3 shall: (a) to the extent possible identify and evaluate available software and hardware patches and updates using automated tools; (b) identify emergency procedures for the patching and updating of ICT assets; (c) test and deploy the software and hardware patches and the updates referred to in Article 8(2), points (b)(v), (vi) and (vii); (d) set deadlines for the installation of software and hardware patches and updates and escalation procedures in case those deadlines cannot be met.
Part II Vulnerability handling requirements Manufacturers of products with digital elements shall: (3) apply effective and regular tests and reviews of the security of the product with digital elements;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_24* *Art. 24, Art. 25, Art. 26 DORA:* 1. For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, shall, taking into account the criteria set out in Article 4(2), establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework referred to in Article 6. 2. The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with Articles 25 and 26. […] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_16* *Art. 16 subparagraph 3 RTS Risk Management* […] 3. The procedure referred to in paragraph 2 shall contain the performance of source code reviews covering both static and dynamic testing. That testing shall contain security testing for internet-exposed systems and applications in

Comments EU-Cyber Resilience Act

	accordance with Article 8(2), point (b), points (v), (vi) and (vii). Financial entities shall: (a) identify and analyse vulnerabilities and anomalies in the source code; (b) adopt an action plan to address those vulnerabilities and anomalies; (c) monitor the implementation of that action plan. 4. […]
Part II Vulnerability handling requirements Manufacturers of products with digital elements shall: (4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_19* *Art. 19 subparagraph 3 DORA:* Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident. In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401774#art_10* *Art. 10 subparagraph 2 RTS Risk Management* The vulnerability management procedures referred to in paragraph 1 shall: […] (e) establish procedures for the responsible disclosure of vulnerabilities to clients, counterparties, and to the public; […]
Part II Vulnerability handling requirements Manufacturers of products with digital elements shall: (5) put in place and enforce a policy on coordinated vulnerability disclosure;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_14* *Art. 14 paragraph 1 DORA:* As part of the ICT risk management framework referred to in Article 6(1), financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.
Part II Vulnerability handling requirements Manufacturers of products with digital elements shall: (6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_14* *Art. 14 paragraph 1 DORA:* As part of the ICT risk management framework referred to in Article 6(1), financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401774#art_8* *Art. 8 subparagraph 2 (c) RTS Risk Management* 2. The policies and procedures for ICT operations referred to in paragraph 1 shall contain all of the following: […] (c) error handling concerning ICT systems, including all of the following:

Comments EU-Cyber Resilience Act

	(i) procedures and protocols for handling errors; (ii) support and escalation contacts, including external support contacts in case of unexpected operational or technical issues; *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774#art_10* *Art. 10 RTS Risk Management, Vulnerability and patch management*
Part II Vulnerability handling requirements Manufacturers of products with digital elements shall: (7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;	Same as Part II (2)
Part II Vulnerability handling requirements Manufacturers of products with digital elements shall: (8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	Same as Part II (2) *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554#art_19* *Art. 19 subparagraph 3 DORA:* Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident. In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking.