NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

ONLINE TRUST COALITION

Legislative Overview

VERSIE 4.0 | LATEST UPDATE February 18 2025

LEGISLATIVE OVERVIEW 3
DISCLAIMER 3
COLOPHON 3
EUROPEAN LEGISLATION IN THE IT SECTOR 4
TIMEFRAME OF LEGISLATION IN SCOPE OF THIS OVERVIEW 5
GDPR GENERAL DATA PROTECTION REGULATION (REGULATION, 2016/679) 6
CSA (EU) 2019/881 CYBERSECURITY ACT (REGULATION, 2019/881) 8
DGA DATA GOVERNANCE ACT (REGULATION, 2022/868) 10
TCO REGULATION ON ADDRESSING THE DISSEMINATION OF TERRORIST CONTENT ONLINE (REGULATION, 2021/784) 12
DSA DIGITAL SERVICES ACT (REGULATION, 2022/2065) 14
NIS2 NETWORK AND INFORMATION SECURITY DIRECTIVE II (DIRECTIVE, 2022/2555) 16
CER CRITICAL ENTITIES RESILIENCE DIRECTIVE (DIRECTIVE, 2022/2557) 19
DA DATA ACT (REGULATION, 2023/2854) 21
AI ACT ARTIFICIAL INTELLIGENCE ACT (REGULATION, 2024/1689) 23
EIDAS (1.0 AND 2.0) ELECTRONIC IDENTIFICATION AND TRUST SERVICES (REGULATION, 2024/1183) 25
CRA CYBER RESILIENCE ACT (REGULATION, 2024/2847) 27
CSAM REGULATION ON PREVENTING AND COMBATING CHILD SEXUAL ABUSE (REGULATION, 2021/1232) 30
CSA (EU) 2023/0109 CYBER SOLIDARITY ACT (REGULATION, PROPOSAL) 32
DMA DIGITAL MARKETS ACT (REGULATION, 2022/1925) 34
CSRD CORPORATE SUSTAINABILITY REPORTING DIRECTIVE (DIRECTIVE, 2022/2464) 36
DORA DIGITAL OPERATIONAL RESILIENCE ACT (REGULATION 2022/2554) 38
CSDDD CORPORATE SUSTAINABILITY DUE DILIGENCE DIRECTIVE (DIRECTIVE, 2024/1760) 40
NPLD NEW PRODUCT LIABILITY DIRECTIVE (DIRECTIVE, 2024/2853) 42

Legislative overview

This overview provides a general insight into current and future legislation of the European Union, which prepares Europe for the digital future. The European approach, which aims to give Europe's citizens, businesses and governments control over the digital transformation, is based on three pillars, namely: technology that works for the people, a fair and competitive digital economy and an open, democratic and sustainable society.

This legislative overview does not comprise all present and future legislation. The purpose of this publication is to provide an overview of those regulations that are currently the most relevant for organization's digital compliance efforts. Completeness was not the objective of this publication. Furthermore this publication was written from a Dutch perspective meaning that reference to national implementing acts, supervisory authorities and examples relate to the Netherlands.

This document is an initiative of the Online Trust Coalition and NOREA. The Online Trust Coalition is a public and private partnership at the initiative of the Dutch Ministry of Economic Affairs. Its purpose is to make trust more tangible. This is done by providing better understandable and interpretable information on security and resilience of systems and services, and more cost effective and less disruptive ways to prove their trustworthiness. NOREA is the Dutch professional organization of Registered IT (EDP) Auditors. NOREA's objective is to promote the quality of professional practice by IT-auditors and to promote their common interest. Registered IT-auditors are, based on their education and experience, the designated experts to carry out IT-assurance assignments. NOREA is partner in the Online Trust Coalition.

Disclaimer:

The reader of this legislative overview cannot derive any rights from the information provided herein. It is not a complete overview, but serves as a guideline for cloud service providers, users of cloud services and supervisory authorities dealing with various European legislation. It is important to note that only a limited selection of relevant legislation is shown and that there are many sector-specific and/or service-specific European laws that are not included. Moreover, this overview focuses on certain aspects of the legislation, without being fully exhaustive on the topics covered. Parts of this legislative overview may be subject to change, therefore this overview is updated from time to time. Always consult the most recent version.

Colophon:

European Legislation in the IT Sector

In the rapidly evolving world of information technology (IT), European legislation is crucial to keep pace with technological advancements and ensure the protection of individuals' rights. Currently, there is a multitude of European legislation in this field, with ongoing development to meet the continuously changing needs of society.

The process of creating European legislation involves several key steps:

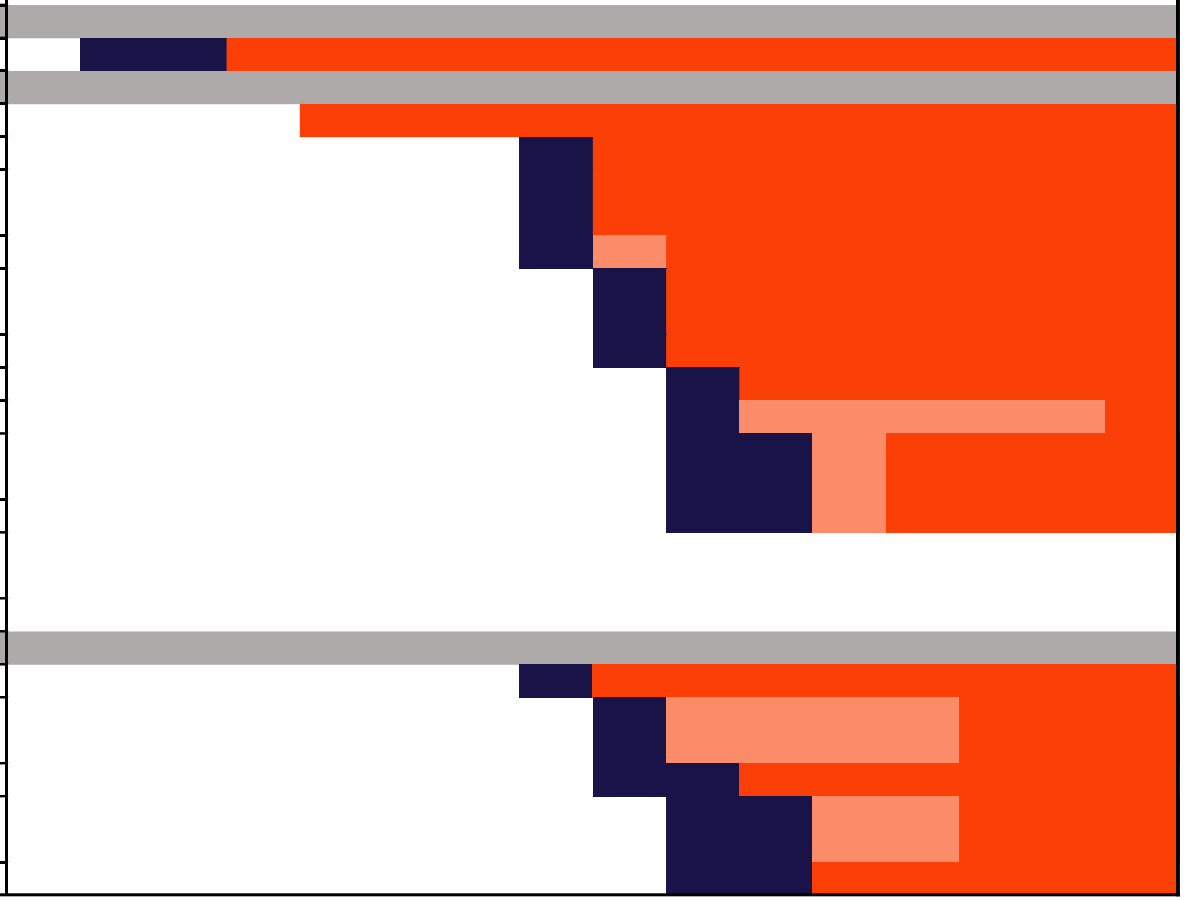
- **Proposal Phase:** Typically initiated by the European Commission, the executive branch of the European Union, this process begins with a proposal. The proposal can originate from various sources, including requests from member states, interest groups, or the Commission's own priorities.
- **Assessment and Amendment:** The proposal undergoes assessment and amendments by both the European Parliament and the Council of the European Union. During this phase, trilogue negotiations occur—an informal process where compromises are reached on specific aspects of the legislative proposal. This allows the institutions to achieve consensus before adopting a final version of the legislation.
- **Approval:** Once agreement is reached between the European Parliament and the Council of the European Union, the law is adopted. Depending on the type of legislation, it may be adopted by qualified majority, unanimity, or, in some cases, with the consent of all member states.
- **Implementation in Member States (with Comitology):** After approval, member states must implement the legislation into their national legal systems. During this process, the European Commission may utilize committees of representatives from member states—such as management committees and regulatory committees—to assist with specific tasks and ensure consistent application and enforcement of the legislation across all member states.

The impact of different European legislation varies depending on its type:

- **Regulations:** Regulations have direct effect in all member states without requiring national implementation. They automatically and immediately apply within the national legal frameworks of all member states, ensuring uniformity across the EU.
- **Directives:** Directives, on the other hand, require national implementation. Each member state must adopt national legislation to meet the objectives of the directives, but they have the freedom to choose specific means and methods to achieve these goals. As a result, implementation may vary slightly among member states, leading to differences in national laws and practices.
- **Recommendations:** Although non-binding, recommendations serve as instruments for the EU to provide guidance to member states on specific issues. They do not have direct legal consequences but can inform national policy-making and practices.

Timeframe of legislation in scope of this overview | Version 4.0 | Last updated on Febuary 18, 2025

Name (abb.)	Name (full)	In force	Applicable from
Data Protection			
GDPR	General Data Protection Regulation (Regulation, 2016/679)	2016	2018
Digital strategy			
CSA	Cybersecurity Act (Regulation, 2019/881)	2019	2021
DGA	Data Governance Act (Regulation, 2022/868)	2022	2023
TCO	Regulation on addressing the dissemination of terrorist content online (Regulation, 2021/784)	2022	2023
DSA	Digital Services Act (Regulation, 2022/2065)	2022	2023
NIS2	Network and Information Security Directive II (Directive, 2022/2555)	2023	2024
CER	Critical Entities Resilience Directive (Directive, 2022/2557)	2023	2024
DA	Data Act (Regulation, 2023/2854)	2024	2025
AIA	Artificial Intelligence Act (Regulation, 2024/1689)	2024	2025
EIDAS 2.0	Electronic Identification and Trust Services (Regulation, 2024/1183)	2024	2026
CRA	Cyber Resilience Act (Regulation, 2024/2847)	2024	2026
CSAM	Regulation on preventing and combating child sexual abuse (Regulation, 2021/1232)	TBA	TBA
CSA	Cyber Solidarity Act (Regulation, proposal)	TBA	TBA
Business, Economy, Euro			
DMA	Digital Markets Act (Regulation, 2022/1925)	2022	2023
CSRD	Corporate Sustainability Reporting Directive (Directive, 2022/2464)	2023	2024
DORA	Digital Operational Resilience Act (Regulation 2022/2554)	2023	2025
CSDDD	Corporate Sustainability Due Diligence Directive (Directive, 2024/1760)	2024	2026
NPLD	New Product Liability Directive (Directive, 2024/2853)	2024	2026



Legend:	
	Legislation is not yet entered into force and is not yet applicable / not yet implemented
	Legislation has entered into force but is not yet applicable / not yet implemented
	Legislation has entered into force and is partially applicable
	Legislation has entered into force and is fully applicable

GDPR
General Data Protection Regulation (Regulation, 2016/679)

Source
http://data.europa.eu/eli/reg/2016/679/oj

Target group
Organizations located inside or outside the EU that process personal data of individuals within the EU.

Applicable from
The Dutch implementation of the GDPR is the General Data Protection Regulation (AVG). The AVG entered into force on May 25, 2018.

Impact
The GDPR/AVG is a European law that protects the privacy of individuals by establishing rules for the processing of personal data. The AVG formulates the principles for the processing of personal data, namely:
- Lawfulness, fairness and transparency: Personal data must be processed in a lawful, fair and transparent manner. This means that the processing must be based on a valid legal basis, must be fair to the data subjects and that they must be aware of how their data is being processed.
- Purpose limitation: Personal data may only be collected and processed for specific, explicit and legitimate purposes. They may not be further processed in a way that is incompatible with these purposes.
- Data minimization: The processing of personal data must be limited to what is necessary for the purposes for which they are processed. Organizations must strive to collect only the data that is strictly necessary.
- Accuracy: Personal data must be accurate and up to date. Appropriate measures must be taken to ensure that inaccurate data is corrected or deleted as quickly as possible.
- Storage limitation: Data may not be kept longer than necessary for the purposes for which they are processed. Organizations must have a policy for the retention periods of personal data.
- Integrity and confidentiality: Personal data must be processed in a manner that ensures adequate security. This includes protection against unauthorized access, loss, destruction or damage.

The AVG imposes obligations on organizations that process such data and determines the rights of data subjects regarding their personal data. If one party is going to process personal data on behalf of the other party, it is important to clarify the role division between parties and, depending on this, to conclude an agreement, such as a data processing agreement.
Link to the AP website for more information: https://www.autoriteitpersoonsgegevens.nl/

Supervision and enforcement (NL and EU)
The supervisory authority for the GDPR (General Data Protection Regulation) in the European Union (EU) is the European Data Protection Board (EDPB). This body ensures that the GDPR is consistently enforced across all EU member states. The EDPB is composed of representatives from national supervisory authorities and coordinates and facilitates cooperation between these authorities.
In the Netherlands, the supervisory authority is the Dutch Data Protection Authority (AP). The AP is authorized to impose sanctions if an organization violates privacy legislation. The main sanctions are the fine, the order subject to a penalty, the processing ban, the reprimand and the warning. A fine is a maximum of 20 million euros or 4% of global annual turnover. In Europe, the EDPS is the supervisory

authority that ensures that European institutions themselves comply with data protection rules and handles complaints about this.

Considerations for IT risk professionals and auditors

Services relevant to IT risk in the context of the GDPR:
-Third-party assurance
Independent audits verify that personal data processing activities comply with GDPR requirements, including data protection and security measures.
-Compliance services
Advisory and support services help organizations ensure adherence to GDPR obligations, such as lawful data processing, consent management, and data subject rights.
-Certifications
Certification services confirm that an organization's data protection policies and practices meet GDPR standards for security, transparency, and accountability.

Consideration for implementation (NL)

No considerations identified

Interfaces with other legislation

None

CSA (EU) 2019/881 Cybersecurity Act (Regulation, 2019/881)

Source
http://data.europa.eu/eli/reg/2019/881/oj

Target group
The CSA primarily applies to all ICT products, ICT services and ICT processes, and their manufacturers or providers, as relevant. An ICT product refers to an "element or a group of elements of a network or information system", such as IoT hardware or software package. An ICT service is a "service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems". An ICT process is described as a "set of activities performed to design, develop, deliver or maintain an ICT product or ICT service".

Applicable from
The CSA (EU) 2019/881 entered into force on June 27, 2019. Most rules have been applicable from June 28, 2021. By now, all rules are applicable.

Impact
The CSA's main objective is to improve cybersecurity in Europe by establishing technical requirements, standards and procedures for ICT products, services and processes. Manufacturers and providers initially have the option to voluntarily opt for cybersecurity certification or an EU declaration of conformity. However, other EU legislation, such as the NIS2 Directive, may mandate certification under the Cybersecurity Act. Importantly, each EU member state has the discretion to determine to what extent certification is mandatory within its jurisdiction, leading to potentially varied implementation across the different member states.
The CSA defines three possible assurance levels, depending on the likelihood and impact of an incident related to an ICT product, service or process during its intended use. These levels are intended to indicate how well a product, service or process should be protected against cyberattacks, with higher levels providing more protection.
In addition to establishing these certification schemes, the CSA also strengthens the mandate of ENISA, the European Union Agency for Cybersecurity. ENISA gets an important role as the European cybersecurity agency and will develop certification schemes on behalf of the European Commission. These schemes, also called certification schemes, are transferred to the European Commission, which then converts them into European regulations.
Infringements of European cybersecurity certification schemes are sanctioned under national law. This ensures an adequate legal framework to ensure compliance and punish any violations, thereby strengthening the effectiveness of the certification schemes and improving cybersecurity in Europe.
Link to ENISA: https://www.enisa.europa.eu/topics/certification/?tab=details

Supervision and enforcement (NL and EU)
The CSA requires each EU Member State to designate at least one National Cybersecurity Certification Authority (NCCA). In the Netherlands, the role of NCCA is fulfilled by the National Inspectorate for Digital Infrastructure, which is part of the Ministry of Economic Affairs and Climate. In the Netherlands, the EU Cybersecurity Act has been implemented through the Cybersecurity Act Implementation Act, which includes additional provisions for the 'high' assurance level and enforcement. Violations can lead to measures by the Minister, fines, penalty payments or withdrawal of certification.

Considerations for IT risk professionals and auditors

No considerations identified

Consideration for implementation (NL)

No considerations identified

Interfaces with other legislation

The certification schemes designed by ENISA are based on designs prepared in close cooperation with experts from industry and Member States, after technical and legal discussions, as well as a public consultation. The schemes will complement the Cyber Resilience Act which introduces binding cybersecurity requirements for all hardware and software products in the EU. This important step contributes to promoting Europe's global digital leadership.
Certification in accordance with the CSA schemes is voluntary, but may be made mandatory under NIS2.

DGA
Data Governance Act (Regulation, 2022/868)

Source
http://data.europa.eu/eli/reg/2022/868/oj

Target group
Public bodies, providers of data intermediation services, data altruism organizations.

Applicable from
The DGA has been applicable since September 24, 2023. Providers of data intermediation services have until September 24, 2025 to comply with their obligations under the DGA.

Impact
The DGA introduces new rules for data intermediation services that focus on sharing data between data holders and data users. Providers of these services must, among other things, comply with security and interoperability requirements. In addition, the DGA contains a framework for data altruism: the processing of data for the public interest. Organizations engaged in this must comply with requirements to protect the privacy and other interests of individuals and companies that make data available. The DGA also contains additional rules to improve the availability of government information.

Supervision and enforcement (NL and EU)
The Authority for Consumers and Markets (ACM) will be the supervisory authority for compliance with the DGA in the Netherlands. Data intermediation services will also have to register with them. Companies, organizations and institutions that are involved in processing data must register with the intended supervisory authority ACM if they want to continue offering their services in the EU.

Considerations for IT risk professionals and auditors
Services relevant to IT risk in the context of the DGA:
-(Legal) consultancy
Advisory services provide guidance on the legal and regulatory reasoning behind whether data can or cannot be shared under the DGA.
-Third-party reporting and assurance
Independent verification of measures related to data anonymization, ensuring compliance with data protection requirements.
-Exchange protocols and control
Assurance services support the implementation, monitoring, and control of secure data exchange protocols in line with the DGA standards.

Consideration for implementation (NL)
The Dutch implementation of the DGA is established through the Uitvoeringswet Datagovernance Verordening (UDGV). The main objective of this law is to set out the rules for the implementation of the DGA in the Netherlands. It creates a framework for data services and defines the role of "data intermediaries" (data brokers) who facilitate data sharing and exchange.
Companies, organizations and institutions in the Netherlands that are involved in processing data can already do a pre-registration with the ACM. This can be done via this website: https://www.acm.nl/nl/online-platforms/datadiensten.

Interfaces with other legislation None

TCO
Regulation on addressing the dissemination of terrorist content online (Regulation, 2021/784)

Source
http://data.europa.eu/eli/reg/2021/784/oj

Target group
Providers of hosting services in the EU, regardless of whether they have their main establishment in the EU Member States.

Applicable from
On June 7, 2022, the (EU) 2021/784 entered into force. This regulation has been implemented in the Netherlands in the "Implementation Act regulation on terrorist content online". The implementation has been in effect since September 1, 2023.

Impact
This regulation aims to tackle the spread of terrorist content online."Terrorist content" means material that incites or solicits the commission of, or contribution to the commission of, terrorist offences, that encourages participation in activities of a terrorist group, or that glorifies terrorist activities, including material depicting a terrorist attack. The definition should also include material that provides instructions for making or using explosives, firearms or other weapons or harmful or dangerous substances, as well as chemical, biological, radiological and nuclear substances (CBRN substances), or for other specific methods or techniques, including the selection of targets, for committing or contributing to the commission of terrorist offences. Such material includes text, images, sound recordings and videos, as well as the live streaming of terrorist offences, thereby creating the risk that more such offences may be committed. In assessing whether material constitutes terrorist content within the meaning of this Regulation, competent authorities and hosting service providers should take into account factors such as the nature and wording of statements, the context in which the statements were made and their potential to lead to harmful consequences for the safety and security of persons. Hosting service providers exposed to terrorist content must include provisions in their terms and conditions - if they have them - to prevent the misuse of their services for the dissemination of terrorist content. They must apply those provisions in a diligent, transparent, proportionate and non-discriminatory manner. The hosting service provider must report to the competent authority on the specific measures so that the competent authority can assess whether the measures are effective and proportionate and whether, if automated means are used, the hosting service provider has the necessary capacities for human oversight and verification.
Hosting service providers are obliged to remove terrorist content identified in the removal order or disable access to it in all Member States within one hour of receiving the removal order.

Supervision and enforcement (NL and EU)
The Authority for Online Terrorist and Child Pornographic Material (AOTKM) can issue removal orders, assess these orders, oversee specific measures and impose sanctions. This AOTKM can exchange data and coordinate and cooperate mutually, and where appropriate with Europol. The financial sanctions imposed, such as a penalty payment, can amount to up to 4% of the global turnover of the hosting service provider in the preceding financial year.

Considerations for IT risk professionals and auditors

No considerations identified

Consideration for implementation (NL)

The Dutch implementation of the TCO regulation is called "Uitvoeringswet Verordening Terroristische online-inhoud".

Interfaces with other legislation

Both regulations (TOI-Vo and SMK-Vo) stipulate that hosting service providers must remove specific unwanted content at the request of a law enforcement authority within a certain (relatively short) period of time.

DSA Digital Services Act (Regulation, 2022/2065)	Source http://data.europa.eu/eli/reg/2022/2065/oj

Target group

Providers of intermediary services (online intermediaries), being mere conduit, caching, and hosting services. Think of internet access providers, cloud service providers, online platforms where users exchange information (social media), online trading platforms where supply and demand are brought together (Marktplaats, Bol.com) and online search engines (Google, Bing).
Not all provisions of the DSA apply to all of the above-mentioned providers.

Applicable from

The DSA has been implemented in stages. Since August 25, 2023, stricter obligations apply to the 19 largest platforms and search engines (with an average of more than 45 million active users per month in the EU).
Since February 17, 2024, the DSA applies to all intermediary services, regardless of their size.

Impact

The DSA clarifies liability rules and introduces due diligence obligations for online intermediaries. It involves an asymmetric package of obligations: there are general rules and specific rules for, for example, online platforms that bring together consumers and traders. The greater the impact a party can have as an intermediary service on consumers and society, the larger and heavier the obligations that must be met.
According to the DSA, certain online intermediaries must tackle illegal content and online disinformation in a targeted manner, possibly adjust content recommendation systems, arrange organizational matters (such as responding to and communicating about illegal content), comply with reporting and information obligations (such as annually assessing the risks of harmful online practices on their services), provide information on specific topics and procedures in the terms and conditions, introduce contact points for authorities and consumers.

Supervision and enforcement (NL and EU)

The European Commission will, in cooperation with national authorities, coordinate the enforcement of legislation, with special attention to compliance by online platforms within their respective jurisdictions. The Commission will primarily be responsible for overseeing and enforcing additional obligations for very large online platforms and search engines. These obligations include, among others, measures to mitigate systemic risks. In the Netherlands, the Authority for Consumers and Markets (ACM) and the Dutch Data Protection Authority (AP) will supervise the DSA.
Member States must ensure that the sanctions for non-compliance with the regulation do not exceed 6% of the annual income or turnover of intermediary service providers, while sanctions for providing incorrect information, not responding to corrections or on-site inspections may not exceed 1% of the annual income or turnover of the service provider concerned.

Considerations for IT risk professionals and auditors

No considerations identified

Consideration for implementation (NL)

The Dutch implementation of the DSA is established through the Uitvoeringswet Digitale Diensten Verordening (UDSV). This law provides the legal basis for the enforcement of the DSA in the Netherlands. It outlines the roles and responsibilities of supervisory authorities, such as the Autoriteit Consument & Markt (ACM) and the Commissariaat voor de Media, in monitoring compliance with the DSA's obligations.

The UDSV aims to increase transparency and accountability of online platforms, protect users' rights, and ensure the swift removal of illegal content. It also introduces stricter rules for advertising transparency and algorithmic accountability, with the possibility of imposing fines or other sanctions on non-compliant platforms.

Interfaces with other legislation

The DSA regulates how online intermediaries should handle reports of allegedly illegal information within their services. For online trading platforms, where supply and demand come together, design requirements apply. The DSA therefore has interfaces with the obligation of hosting services to remove content related to sexual abuse of children and/or of a terrorist nature ((EU) 2021/784 and (EU) 2022/209) and the design requirements that specifically apply to online marketplaces (DIRECTIVE 2011/83/EU).

NIS2
Network and Information Security Directive II (Directive, 2022/2555)

Source
http://data.europa.eu/eli/dir/2022/2555/oj

Target group
Important and essential entities active in highly critical sectors or other critical sectors.
According to NIS2, the following sectors fall under "Sectors of high criticality": energy; transport; banking; financial market infrastructures; health; digital infrastructure; drinking water; waste water; digital infrastructure; ICT service management (business-to-business); public administration and space. "Other critical sectors" are: postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; manufacturing; digital providers and research.
An entity is considered important when it:
• Is active in a highly critical sector and is a "medium-sized" organization of 50 – 249 persons with an annual turnover of €10 million to €50 million or a balance sheet total of €10 - €43 million.
or
• Is active in a sector mentioned in another critical sector; and is a "large" or "medium-sized" organization based on the above-mentioned criteria.
An entity is considered essential when it:
• Is active in a highly critical sector; and is a "large" organization of 250 persons or more, or has an annual turnover of more than €50 million and a balance sheet total above €43 million.
Furthermore, parties can also be essential if they are designated on other grounds.

Applicable from
The NIS2 is applicable from January 16, 2023. European Member States have until October 17, 2024 to align their national laws and regulations with the directive.

Impact
NIS2 imposes, among others, the following obligations:
- Registration obligation: entities must register with the competent authority, including Chamber of Commerce details and IP addresses.
- Reporting obligation: Companies and government organizations falling under NIS2 must report incidents that can cause significant disruption of essential services to the supervisory authority within 24 hours. In addition, cyber incidents must be reported to the Computer Security Incident Response Team (CSIRT), which can then provide support. Factors that make an incident reportable include the number of affected persons, the duration of the disruption, and potential financial losses.
- Duty of care: The directive requires entities to conduct their own risk assessment. Based on this, they must take appropriate measures to ensure the continuity of their services and safeguard the security of the information used. Measures for managing cyber and security risks include, for example: risk analyses, incident handling, business continuity, supply chain security, security in data processing, developing and maintaining network and information systems, establishing policies and procedures to assess the effectiveness of cybersecurity risk management measures, basic practices in cyber hygiene and training in cybersecurity, policies on the use of cryptography and encryption, security aspects for personnel, access policy and asset management, when appropriate, use of MFA or continuous authentication solutions, secure voice, video and text communication, and secure emergency and communication systems within the organization.

- Governance: directors must be more involved in their organization's cybersecurity. Directors must pay attention to their level of knowledge of cybersecurity by taking training.
It's important to note that not all provisions of the NIS2 directive apply to every party. For example, the registration obligation is very limited in application (depending on the nature of the services a party provides), a healthcare provider does not need to register, but a DNS service provider does.

Supervision and enforcement (NL and EU)

The primary supervisor in the Netherlands will be the Rijksinspectie Digitale Infrastructuur (RDI). The RDI directly supervise many sectors like: energy, digital infrastructure, space, and government services. Some other sectors with essential service providers, like the financial sector, already have active and dominant supervisors and specific cyber regulations. To avoid a repetition of reporting requirements, supervision on NIS2 remains at the sector specific supervisor. These are: Autoriteit Nucleaire Veiligheid en Stralingsbescherming, Autoriteit Persoonsgegevens, De Nederlandsche Bank, Inspectie Gezondheidszorg en Jeugd, Inspectie Leefomgeving en Transport, Inspectie Justitie en Veiligheid.

Member States must ensure that the supervisory authority has, among other things, the ability to issue binding instructions and orders, and to impose administrative fines. The maximum amount of these fines must be set by the Member States at a maximum of €10 million or 2% for essential entities and a maximum of €7 million or 1.4% for important entities of the total worldwide turnover, whichever is higher. Moreover, directors can be held liable if they do not comply with the NIS2 directive.

Considerations for IT risk professionals and auditors

IT Risk Management itself is an important element within the directive. Services related to the setup, certification and assurance can therefore be relevant. It should also be noted that service providers towards organisations that are considered vital may differentiate themselves when able to prove their competence in risk management and reporting. Associated standards like the cyber security conformity certification, ISO 27001 and the NOREA's Reporting Initiative may provide futher guidance.
Compliance with existing information security frameworks in government, including the "Baseline Informatiebeveiliging Overheid (BIO)", that applies in the Netherlands, serves as a basis for fulfilling the duty of care arising from NIS2. Compliance with current obligations thus forms a crucial starting point. For government agencies, this means that the fulfillment of the NIS2 duty of care will take place as much as possible within the boundaries of existing frameworks. Organizations that previously did not comply with existing information security frameworks now have the obligation to do so under NIS2.

Consideration for implementation (NL)

In the implementation of the NIS2 directive in the Netherlands, certification will not be made mandatory. Instead, the focus is on encouraging organizations to take appropriate measures to improve their digital resilience. This approach provides flexibility, allowing companies and institutions to tailor their security measures to their specific risks and needs without being bound by a mandatory certification process.
In the Netherlands, the current Wet beveiliging netwerk- en informatiesystemen (Wbni) and the associated Besluit beveiliging netwerk- en informatiesystemen (Bbni) are currently in force. These will expire once the Cybersecuritywet (Csw), which implements the NIS2 directive, comes into effect. Csw is expected to take effect in the third quarter of 2025. During the transition period, full obligations like the duty of care and reporting requirements are not yet in force, but organizations do have some rights due to the direct effect of certain provisions of the directive. The National Cyber Security Centre (NCSC) is already carrying out several tasks assigned under the Cbw, such as system monitoring, incident management, and issuing warnings. From October 17, 2024, organizations can voluntarily report incidents and register for threat information through the NCSC portal.

The RDI offers a NIS2 self-assessment (https://regelhulpenvoorbedrijven.nl/NIS-2-NL/) to help organizations determine if they fall under the NIS2 directive and their importance. Additionally, the Dutch government provides the NIS2 Quickscan for ICT and cybersecurity specialists (https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/) to assess their organization's digital resilience through 40 yes/no questions.
Certifications (e.g. under Cybersecurity Act) will NOT be mandatory in NL.

Interfaces with other legislation

Between CER and NIS2, there is significant overlap, but there are also differences. Here are the similarities and differences:
Similarities:
-Both directives require collaboration between national authorities to protect critical infrastructure.
-Sectors such as energy, transport, healthcare, and water management are often covered by both directives.
-Both CER and NIS2 impose requirements for risk assessment and risk management, though with different areas of focus.
-Incident reporting is mandatory under both directives: CER for physical or operational disruptions and NIS2 for cyber incidents.
Differences:
-CER focuses on physical and operational resilience, while NIS2 emphasizes cybersecurity.
-CER addresses physical threats (e.g., sabotage, natural disasters), whereas NIS2 deals with cyber threats (e.g., hacking, data breaches).
-CER mandates physical security and continuity measures, while NIS2 emphasizes cybersecurity measures, such as ICT risk management.
-CER is overseen by physical security authorities, while NIS2 is monitored by cybersecurity authorities, such as Computer Security Incident Response Teams (CSIRTs).

CER
Critical Entities Resilience Directive (Directive, 2022/2557)

Source
http://data.europa.eu/eli/dir/2022/2557/oj

Target group
The requirements apply exclusively to institutions designated by the government as critical entities. An entity is considered critical when it provides essential services within the sectors of digital infrastructure (including telecom providers, top-level domain name registers and cloud providers), banking, energy, transport, financial market infrastructure, health, drinking water or wastewater management, public administration, space or the production, processing and distribution of food. Previously designated as 'vital providers' within these sectors will also be recognized as critical entities.

Applicable from
The CER Directive came into force on January 16, 2023. Member States have 21 months to transpose the directive into national legislation.

Impact
The CER Directive is designed to make critical organizations more resilient against physical threats such as terrorist attacks, disasters and climate change. This directive establishes various resilience measures and requires that serious incidents be reported within 24 hours. Organizations can use government-provided risk assessments to determine the appropriate resilience measures. Non-compliance with the implemented CER Directive will be penalized.
The CER Directive imposes a number of essential obligations, including:
- Duty of care - Companies must conduct their own risk assessment and based on that, take measures to ensure the continuity of their services and protect their information against physical threats.
- Reporting obligation - Companies must report incidents that can significantly disrupt essential services to the supervisory authority within 24 hours. In case of a cyber incident, this must also be reported to the Computer Security Incident Response Team (CSIRT), which can then provide help and assistance. Whether an incident falls under the reporting obligation depends on various factors such as the number of affected persons, the duration of the disruption and potential financial losses.
- Supervision - Organizations falling under the CER Directive are placed under supervision to check whether they comply with the obligations of the directive, such as the duty of care and reporting obligation.

Supervision and enforcement (NL and EU)
In case of violation of the duty of care or reporting obligation, the supervisory authority can impose a fine of up to 10,000,000 euros or 2% of global annual turnover, whichever is higher. For other violations, a maximum fine of 1 million euros applies. In addition, the Netherlands must establish rules for imposing sanctions. The supervisor for the Wet weerbaarheid kritieke entiteiten (Wwke), which stems from the Critical Entities Resilience (CER) Directive, will depend in the Netherlands on the specific sector in which the critical entities operate.
For the healthcare sector, the Inspectie Gezondheidszorg en Jeugd (IGJ) will be responsible for oversight and enforcement. For other sectors, such as energy and drinking water supply, critical entities are designated by the relevant ministries, and the responsible supervisory authority can vary depending on the sector. In general, the Rijksinspectie Digitale Infrastructuur (RDI) supervises digital infrastructures and related sectors.

Considerations for IT risk professionals and auditors

IT Risk Management itself is an important element within the directive. Services related to the setup, certification and assurance can therefore be relevant. It should also be noted that service providers towards organisations that are considered vital may differentiate themselves when able to prove their competence in risk management and reporting. Associated standards like the cyber security conformity certification, ISO 27001 and the NOREA's Reporting Initiative may provide futher guidance.

Consideration for implementation (NL)

The CER Directive will be implemented in "Wet weerbaarheid kritieke entiteiten". Between October 17, 2024, and the date this law comes into effect, there are no obligations for organizations under the CER Directive. These obligations will only apply once the Critical Entities Resilience Act is in force and an organization is designated as a critical entity. After this designation, a critical entity will have 10 months to comply with obligations such as the duty of care and the reporting requirement under the CER.
The ministries designate regulators to oversee compliance with the obligations for critical entities, with an emphasis on the duty of care. The Wwke also empowers the regulator to take enforcement measures if these obligations are not adhered to. For instance, the regulator can mandate an audit or require certain actions, and, if necessary, impose administrative enforcement or a fine.

Interfaces with other legislation

Between CER and NIS2, there is significant overlap, but there are also differences. Here are the similarities and differences:
Similarities:
-Both directives require collaboration between national authorities to protect critical infrastructure.
-Sectors such as energy, transport, healthcare, and water management are often covered by both directives.
-Both CER and NIS2 impose requirements for risk assessment and risk management, though with different areas of focus.
-Incident reporting is mandatory under both directives: CER for physical or operational disruptions and NIS2 for cyber incidents.
Differences:
-CER focuses on physical and operational resilience, while NIS2 emphasizes cybersecurity.
-CER addresses physical threats (e.g., sabotage, natural disasters), whereas NIS2 deals with cyber threats (e.g., hacking, data breaches).
-CER mandates physical security and continuity measures, while NIS2 emphasizes cybersecurity measures, such as ICT risk management.
-CER is overseen by physical security authorities, while NIS2 is monitored by cybersecurity authorities, such as Computer Security Incident Response Teams (CSIRTs).

DA Data Act (Regulation, 2023/2854)	Source https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1732695799856

Target group

Providers of data processing services. This includes providers of cloud and edge services.

Applicable from

The DA entered into force on January 11, 2024. Companies have time to prepare, as the DA will become applicable from September 2025.

Impact

The DA must provide a uniform framework for the use and sharing of data throughout the EU.
Additional explanation follows:
- The DA imposes specific rules on companies that collect data or sell smart devices. The emphasis is on transparency, access to data, the possibility to switch between cloud services, the government's authority to demand data, and provisions in contracts.
- A crucial aspect of the DA is the obligation for manufacturers and sellers to provide transparency to consumers. Products and services should be designed so that generated data is easily and safely accessible by default. Consumers have the right to obtain this data free of charge and can choose to share it with third parties, with restrictions to prevent misuse.
- In addition, the Data Act focuses on facilitating the switch between cloud services, with large providers such as Google and Apple having to ensure functional equivalence. Although a fee is allowed in the first three years, switching should be free thereafter.
- In special situations, the government can demand data, with clear criteria for emergency situations or tasks of general interest (see chapter 5).
- The DA also affects contractual provisions, imposing obligations regarding switching to other services and prohibiting clauses that are contrary to good trading practices.
- Regarding interoperability requirements, the DA requires operators of data spaces to be compatible with other data spaces, including descriptions of data structures, formats and technical access.

Supervision and enforcement (NL and EU)

Each country within the EU must designate one or more authorities responsible for implementing and enforcing this regulation. They can choose to designate existing authorities or establish new authorities. The Authority for Consumers & Markets (ACM) and the Dutch Data Protection Authority (AP) have been designated as national supervisory authorities.
The supervisory authorities can impose fines for violations of this regulation up to €20,000,000 or 4% of the total worldwide annual turnover in the previous financial year.
Specifically for violations related to making data available to government authorities and EU institutions, agencies or bodies due to exceptional necessity, the supervisory authority can impose fines of up to €50,000 per infringement and a maximum of €500,000 per year. Furthermore, Member States can establish additional rules for the penalties that apply to violations of this regulation and take all required measures to ensure that these penalties are enforced.

Considerations for IT risk professionals and auditors

Services relevant to IT risk in the context of the Data Act:

- Third-party assurance

Independent audits provide assurance that data access and sharing practices comply with the requirements of the Data Act.

- Compliance services

Support in ensuring that organizations adhere to the data-sharing obligations, access rights, and security measures mandated by the Data Act.

- Certifications

Certification services verify that data management processes meet the standards for data portability, security, and transparency set by the Data Act.

Consideration for implementation (NL)

No considerations identified

Interfaces with other legislation

The measures proposed in the Data Act complement the measures that were already provided under the Data Governance Act.

See: https://digital-strategy.ec.europa.eu/en/policies/data-act

AI Act Artificial Intelligence Act (Regulation, 2024/1689)	Source https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689&qid=1732693395878

Target group

Providers who place AI systems on the market or put them into service in the EU and providers of AI systems located outside the EU when the output of the AI system is used in the EU. In addition, distributors, importers, users and possibly third parties dealing with AI systems.

Applicable from

The AI Act came into force in August 2024. In February 2025, the rules will apply to AI systems that pose an unacceptable risk. In May 2025, the deadline for providers of general-purpose AI to establish their codes of conduct will be reached.
The general application of the AI Act will begin in August 2026, with high-risk AI systems, as listed in Annex I, still being exempt. Starting in August 2027, the rules will also apply to these high-risk AI systems. Finally, from December 31, 2030, the AI Act will apply to certain large legacy IT systems of European and national governments.

Impact

All use of AI falls under the AI Act. The regulation follows a risk-based approach and imposes obligations on providers and users depending on the risk level that an AI system entails. The AI Act applies to all sectors and is not limited to a specific industry. In broad terms, a distinction is made between AI systems with:
- Unacceptable Risks: If an AI system acts contrary to European fundamental norms and values, it cannot be deployed in the European market. An example of this is predictive policing; using AI to predict if someone will exhibit criminal behavior. However, there is some allowance for biometric surveillance under strict conditions.
- High Risks: AI systems that pose a high risk to health, safety, fundamental rights, or the environment are allowed only if they meet stringent requirements. For instance, the source of the data used to train the AI must be clear, human oversight is required, and technical documentation must be in order. Handling insurance claims, certain medical devices, and algorithms that evaluate job applicants are examples of high-risk AI.
- Low Risks: AI systems that do not fall under the previous categories can enter the European market without much trouble. However, the AI must be transparent, ensuring that no one mistakes it for a human, and the AI cannot make decisions.
- Specific Transparency Risk: General AI models and foundation models such as GPT and Bard.
AI systems with unacceptable risks are prohibited. Most obligations apply to high-risk AI systems, which include:
- Fundamental Rights Impact Assessment: Structured assessment of risks related to safety, privacy, discrimination, fair access to healthcare, education, and essential services must be conducted in advance.
- Risk Management System: Identifying, evaluating, managing, and mitigating potential risks.
- Data Management System: Use of unbiased, qualitative, and representative datasets is required.
- Technical Documentation: Users must clearly understand how to use the AI system.
- Transparency: Users must understand how the AI system works. This includes a logging requirement to trace and verify actions.

- Human Oversight: Human supervision is required during the AI system's operation.
-Conformity Assessment: A specific conformity assessment procedure tailored to the unique characteristics and risks of AI systems, differing from the current CE marking system for other products, is required.
Obligations for Low-Risk AI Systems
Low-risk AI systems will be subject to transparency obligations, among other things.
The aforementioned obligations are not the responsibility of a single party; the AI Act defines different roles, each with its own responsibilities.

Supervision and enforcement (NL and EU)

The AI Act requires that a national supervisory authority be designated by each Member State, which cooperates with national competent authorities to ensure that the AI Act is complied with. This national supervisory authority is part of the European AI Board (EAIB).
In the Netherlands, the Dutch Data Protection Authority (AP) and the Digital Infrastructure Inspectorate (RDI) advise the government to involve market regulators and inspection services in overseeing compliance with the AI Act, with the AP acting as the coordinating supervisory authority. They propose aligning AI supervision with regular oversight in various sectors and domains. However, the government has not yet made a formal decision on this matter.
A national supervisory authority can demand access to all documentation, source code and model parameters, give binding instructions on adjusted use, order cessation if the AI proves to be too risky after all. Moreover, Member States must also establish fines within the limits set in the AI Act. That is €35 million or for companies 7% of worldwide group turnover for the use of prohibited AI, €15 million or for companies 3% of worldwide group turnover for other violations
€7.5 million or for companies 1.5% of worldwide group turnover for providing incorrect information about risk status or for transparency requirements.
Lower ceilings will apply for SMEs and startups.

Considerations for IT risk professionals and auditors

Services relevant to IT risk in the context of the AI Act:
-Declarations of conformity
Organizations must provide declarations of conformity to demonstrate that their AI systems comply with the AI Act.
-Third-party assurance
Independent audits are required for certain high-risk AI systems to ensure compliance and safety.
-Governance consultancy
Consultancy services support the development of policies, risk management, and compliance processes to effectively mitigate IT risks.

Consideration for implementation (NL)

No considerations identified

Interfaces with other legislation

Where the AR aims to protect consumers against damage caused by a defective product (including digital services), the AILD supplements the AR by specifically easing the burden of proof for consumers who have suffered damage from an AI system. The AILD in turn complements the AI Act. By offering consumers a possibility to recover damages caused by, for example, an AI system that has caused unacceptable risks and has not been removed from the European market.

eIDAS (1.0 and 2.0) Electronic Identification and Trust Services (Regulation, 2024/1183)	Source https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183&qid=1732697390044

Target group

Governments and trust service providers

Applicable from

eIDAS 1.0 has been in effect since September 29, 2018, and.eIDAS 2.0 entered into force on May 20, 2024.
The European Commission must first develop so-called implementing acts (IAs), which are technical specifications and procedures for the European Digital Identity Wallet (EUDIW). The first set of IAs must be made publicly available by the end of November 2024 at the latest.
Each member state is required to make at least one national EUDIW available within 24 months after the publication of these IAs, meaning no later than the end of November 2026.
Additionally, so-called relying parties – public and private organizations that are legally or contractually obligated to apply strong user authentication for digital identification – must accept EUDIWs within 36 months of the publication of the IAs. This must be completed by the end of November 2027 at the latest. These relying parties include, among others, banks, payment institutions, electronic money institutions, and other financial institutions.

Impact

The current eIDAS Regulation (1.0) sets uniform requirements for the assurance levels of electronic IDs. In addition, it provides a framework for different types of electronic signatures, including simple, advanced and qualified electronic signatures. The use of electronic signatures requires an analysis of the required type of signature and its suitability for the intended transactions.
The new eIDAS Regulation (2.0) provides all EU citizens with a digital identity through a digital wallet that allows users to identify and authenticate themselves online and offline across borders to access a wide range of public and private services.
This wallet offers an optional digital identity that gives individuals control over their personal data. It can be used as an identification means to provide specific documents. Some examples of the use of this wallet are: accessing a personal bank account or applying for a loan; submitting tax returns and completing enrollments at educational institutions.
Local governments will be obliged to recognize the European digital identity once the associated regulation comes into force. This means that they must ensure the integration of the mentioned means, such as the digital wallet, and new trust services in their service provision, including providing the necessary support.

Supervision and enforcement (NL and EU)

Supervision of eIDAS 1.0 is regulated in the Netherlands in the "Telecommunicatiewet". The supervisory authority is the National Inspectorate for Digital Infrastructure, which falls under the Ministry of Economic Affairs and Climate. It is expected that the new regulation will also fall under this.

Considerations for IT risk professionals and auditors

No considerations identified

Consideration for implementation (NL)

The implementation of the eIDAS 2.0 Regulation in the Netherlands requires adjustments to existing Dutch legislation in the area of electronic identification and trust services. This will likely occur through amendments to the Wet Digitale Overheid (WDO), which provides a framework for the use of electronic identification means and digital access services in the public sector.

The Wet Digitale Overheid regulates the use of national digital identification means (such as DigiD) and is part of the broader European legal framework under eIDAS. To comply with the new requirements of the eIDAS 2.0 Regulation, additional provisions will be added to the WDO, such as enabling the issuance of the European Digital Identity Wallet (EUDI Wallet) to Dutch citizens and ensuring interoperability across the EU.

Further amendments to other laws may also be required to involve the private sector, particularly concerning the acceptance of the EUDI Wallet for identity verification and document signing in various sectors.

Thus, the Wet Digitale Overheid will be a key piece of legislation in aligning Dutch law with the requirements of the eIDAS 2.0 framework.

Interfaces with other legislation

None

CRA Cyber Resilience Act (Regulation, 2024/2847)	Source https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847&qid=1732695048414

Target group

Manufacturers, importers and distributors of products with digital elements that are connected to other devices or a network. The law obliges also national cybersecurity coordinators, such as the National Cyber Security Centre (NCSC), to proactively report incidents and exploitable vulnerabilities. In this way, the CRA seeks to enhance digital resilience across the European Union.

Applicable from

The CRA came into force on December 11, 2024.
The implementation of the CRA will be phased to give manufacturers sufficient time to comply with the new requirements.

- During the first 18 months, from December 11, 2024, to June 11, 2026, the focus will be on the preparatory phase, including the development of harmonized standards.
- On September 11, 2026, the reporting obligation for actively exploited vulnerabilities and incidents will come into force.
- By December 11, 2026, the harmonized standards and notified bodies must be available, enabling products to be assessed for compliance.
- From December 11, 2027, all CRA requirements will apply, and all digital products, software, and apps must fully comply with the new regulations.

Impact

The CRA ensures that digital products, including all hardware (of which certain software is a part), software and components, meet essential cybersecurity requirements before they are placed on the European market.
The CRA imposes strict requirements before they can be marketed. These requirements include:
-Products must be safely designed, developed, and produced (secure-by-design).
-They must not have known exploitable vulnerabilities.
-Default configurations must be secure (secure-by-default).
-Automatic updates must be enabled by default.
-Products must offer strong authentication and authorization, and data must be well protected, for example, through encryption.
-Sensitive data must be minimized, and availability must be ensured, even against DDoS attacks.
Essential security requirements for handling vulnerabilities:
-Manufacturers must identify and document vulnerabilities.
-Vulnerabilities must be addressed immediately with free security updates throughout the product's lifecycle.
-Security must be regularly tested and assessed.
-Vulnerabilities must be publicly disclosed after the availability of a security update.
-Manufacturers must establish policies for coordinated vulnerability disclosure and provide a secure update mechanism.
Reporting obligation:
-Vulnerabilities and security incidents must be actively reported.

-In the event of an incident, an early warning must be given within 24 hours, and a full report of the incident within 72 hours.
Product lifecycle:
-Suppliers must establish and proactively communicate the support period of products at the time of sale, for both digital and physical products.
-Regulators will track and communicate the average expected lifespan of products at an aggregated level.
Digital products that meet these requirements may use the CE marking to offer them in the internal market. In most cases, parties can self-assess whether they meet the requirements. However, for a select group of critical products, an assessment by an external party is required. The specific list of these critical products is still under final negotiation and cannot yet be provided (refer to Annex 3, Class 2).

Supervision and enforcement (NL and EU)

The CRA provides supervisory authorities with powers to impose fines. At this moment, it is not yet known which party will become the supervisory authority in the Netherlands. Non-compliance with crucial obligations regarding cybersecurity can result in fines of up to € 15 million or 2.5% of annual turnover, whichever is higher. For other violations within the CRA, administrative fines of up to € 10 million or 2% of global annual turnover are possible, if that amount is higher. Providing incorrect information to market surveillance authorities can lead to a fine of € 5 million or 1% of global annual turnover in the previous tax year, whichever is higher. Member States have the freedom to impose additional sanctions for non-compliance with the CRA, provided these are proportionate and effective, but they must notify these rules to the European Commission. Market surveillance authorities can prohibit or restrict products if manufacturers, importers, distributors or other responsible companies do not meet the requirements. The European Commission also has the authority to take measures for products with digital components that pose a significant security risk, including recalling or withdrawing these products from the market within a reasonable timeframe.

Considerations for IT risk professionals and auditors

Services relevant to IT risk in the context of the Cyber Resilience Act:
-Change management assurance
Assurance services ensure that changes to IT systems are managed securely and in compliance with the requirements of the Cyber Resilience Act.
-Security testing
Security testing services help identify vulnerabilities and verify that systems meet cybersecurity standards to prevent potential threats.
-Conformity assessments
Independent assessments confirm that IT products and services comply with the security requirements outlined in the Cyber Resilience Act.

Consideration for implementation (NL)

No considerations identified

Interfaces with other legislation

The CRA and the NIS2 share significant overlaps and complement each other in strengthening cybersecurity within the European Union. Both frameworks focus on improving digital security but target different audiences and responsibilities. While the CRA sets requirements for manufacturers of digital products, the NIS2 focuses on providers of essential and important services.
A key intersection is the obligation to report incidents. The CRA requires manufacturers to proactively report exploitable vulnerabilities and incidents, while the NIS2 mandates organizations to report cyber incidents that impact essential services. Additionally, both frameworks emphasize the importance of

effective vulnerability management, requiring both manufacturers and service providers to ensure active monitoring and risk mitigation.
The involvement of national cybersecurity coordinators, such as the National Cyber Security Centre (NCSC), also plays a crucial role in both frameworks. The CRA and NIS2 both call for national oversight and coordination, contributing to stronger digital resilience at both national and European levels.
Together, the CRA and NIS2 provide a complementary framework that marks a significant step towards a more secure digital ecosystem in Europe.

CSAM Regulation on preventing and combating child sexual abuse (Regulation, 2021/1232)	Source http://data.europa.eu/eli/reg/2021/1232/oj

Target group

Providers of hosting services and providers of publicly available interpersonal communications services

Applicable from

The regulation has not yet entered into force. It is unclear when this will happen.

Impact

This regulation aims to require hosting service providers and interpersonal communication service providers to identify, analyze and assess the risk of the service being used for online child sexual abuse for each service they offer. Providers of hosting services and providers of interpersonal communications services identify, analyze and assess for each such service they offer the risk that the service is used for online child sexual abuse. The term "child sexual abuse" should refer not only to the distribution of material previously identified and confirmed to be child sexual abuse material ("known" material), but also to previously unidentified material that is likely to be child sexual abuse material but has not yet been confirmed as such ("new" material), as well as activities amounting to the solicitation of children ("grooming").

Hosting service providers must conduct a risk assessment, implement risk mitigation measures, and the law enforcement authority may require the hosting service provider to take measures (such as installing new technologies) to detect sexual abuse. Furthermore, the provider has a reporting obligation, and a duty to remove the content as soon as possible and in any case within 24 hours after a request from the law enforcement authority.

By establishing a European Centre for the prevention and combating of child sexual abuse ("the EU Centre"), the proposal also aims to help providers reduce their responsibilities. In particular, the EU Centre will set up, maintain and manage databases with indicators of online child sexual abuse, which must be used by providers to comply with their detection obligations.

Supervision and enforcement (NL and EU)

The EU Centre will work closely with the coordinating authority. At this moment, it is not known who will be the coordinating authority in the Netherlands. It is expected that this will be the Authority for Online Terrorist and Child Pornographic Material (AOTKM).

The coordinating authority can issue removal orders, oversee specific measures and impose sanctions. Sanctions for providing incorrect, incomplete or misleading information, for failing to respond, failing to rectify incorrect, incomplete or misleading information or refusing to submit to an on-site inspection, shall not exceed 1% of the provider's annual income or total turnover.

Other financial sanctions can amount to up to 6% of the global turnover of the hosting service provider.

Considerations for IT risk professionals and auditors

No considerations identified

Consideration for implementation (NL)

The Dutch implementation of the CSAM is called "Verordening ter voorkoming en bestrijding van seksueel misbruik van kinderen".

Interfaces with other legislation

Both regulations (TOI-Vo and SMK-Vo) stipulate that hosting service providers must remove specific unwanted content at the request of a law enforcement authority within a certain (relatively short) period of time.

CSA (EU) 2023/0109
Cyber Solidarity Act (Regulation, proposal)

Source
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209

Target group
Entities active in highly critical sectors (healthcare, transport, energy, etc.) may be subject to so-called 'coordinated preparedness tests'. In addition, it is possible to participate in the EU Cybersecurity Reserve.

Applicable from
The Council adopted the text on December 2, 2024, but a formal signature and publication in the Official Journal are required before the act can come into force.

Impact
The purpose of this regulation is to strengthen the capacity within the EU to detect, prepare for and respond to significant and large-scale cyber threats and attacks. The proposal includes the establishment of a European cybersecurity shield, consisting of interconnected operational security centers across the EU, and a comprehensive cybersecurity emergency mechanism to improve the EU's cyber resilience. The European cyber shield will be built from Security Operations Centers (SOCs) spread across the EU, grouped in various multi-country SOC platforms, funded with support from the Digital Europe Program (DEP) alongside national funding. The Cyber Shield will be responsible for improving the detection, analysis and response to cyber threats. These SOCs will deploy advanced technologies such as artificial intelligence (AI) and data analysis to detect and share warnings of such threats with authorities across borders. The cyber emergency mechanism aims to improve preparedness and response to cyber incidents through three main actions:
-Testing critical sectors (such as healthcare, transport and energy) for possible weaknesses in their cybersecurity, based on a common risk assessment at EU level.
-The establishment of an EU cybersecurity reserve, consisting of incident response services from private service providers, which can be deployed at the request of Member States or EU institutions to address significant or large-scale cybersecurity incidents.
-Providing mutual assistance between Member States to support each other in addressing cybersecurity incidents.
The proposed regulation also includes the establishment of a mechanism for the evaluation of cybersecurity incidents, with the aim of assessing and evaluating specific incidents. At the request of the Commission or national authorities (the EU-CyCLONe network or the CSIRT network), ENISA will be responsible for assessing specific significant or large-scale cybersecurity incidents with regard to cybersecurity. ENISA must prepare a report with lessons and, where applicable, recommendations for improving the EU's cyber response.

Supervision and enforcement (NL and EU)
Supervision currently unknown

Considerations for IT risk professionals and auditors

No considerations identified

Consideration for implementation (NL)

No considerations identified

Interfaces with other legislation

The CSA (EU) 2023/0109 complements and supports structures under other cybersecurity instruments, such as the NIS2 Directive or CSA (EU) 2019/881. This complementation and support consists of taking effective measures and cooperating loyally, efficiently, solidarily and in coordination with each other, the Commission and other relevant public authorities as well as the entities concerned to make critical infrastructure used to provide essential services in the internal market more resilient.

DMA
Digital Markets Act (Regulation, 2022/1925)

Source
http://data.europa.eu/eli/reg/2022/1925/oj

Target group
Gatekeepers providing core platform services. A platform falls under the DMA as a gatekeeper if it provides the same core platform service in at least 3 EU member states and has achieved an annual turnover of € 7.5 billion in the EU in the last 3 years or if it has a market value of at least € 75 billion in the previous year. Such a platform must also have at least 45 million active end users and at least 10,000 business users established in the EU for 3 years.
As of September 6, 2023, 6 gatekeepers and 22 of their services have been designated: Alphabet (with services such as Google Search and YouTube), Amazon, Apple (including the App Store), ByteDance (TikTok), Meta (including Facebook and WhatsApp), and Microsoft (including Windows and LinkedIn).

Applicable from
The DMA entered into force on November 1, 2022. As of May 2, 2023, the DMA is also actually applicable.

Impact
The DMA contains additional competition rules for a limited number of online platforms that have a very large market share. These platforms have such a position that they effectively function as 'gatekeepers' for the internet: as an entrepreneur, you can hardly avoid these platforms. For the gatekeepers, additional rules apply to ensure fair access to and use of their services. Some examples of what gatekeepers must do: offer fair conditions to entrepreneurs when they offer apps in the platform's app store, give entrepreneurs free access to their own data (including customer data) upon request, give entrepreneurs access to data on how well their advertisements perform on the platform, ensure that apps and payment services of entrepreneurs can connect to (be interoperable with) the gatekeeper's operating system and hardware.
Some examples of what gatekeepers are not allowed to do: prohibit entrepreneurs from offering products or services on their own website or another platform at a lower price or with better conditions (this is also called a parity clause), favor their own products and services or treat them better than comparable products or services from entrepreneurs in the search results, require entrepreneurs to use certain additional services (such as using the gatekeeper's payment service for in-app purchases), use data that the platform collects from entrepreneurs with one service in competition with that entrepreneur in another service (for example in digital advertising), prevent entrepreneurs from communicating with customers and offering subscriptions outside the app store.

Supervision and enforcement (NL and EU)
The Commission has the primary role in enforcing the DMA. In addition to conducting market research, the European Commission also gets various investigative powers, such as requesting information and carrying out inspections. Furthermore, the Commission can take interim measures and, after presenting preliminary findings, impose both behavioral measures and substantial fines and periodic penalty payments for violations of the DMA. These fines can amount to 10% of global turnover, and even more than 20% for repeat offenders. For repeated violations within eight years, the Commission can also impose structural measures after market research, such as temporary bans on new mergers.

National authorities have a supporting role in monitoring compliance with the DMA. In the Netherlands, the Authority for Consumers and Markets ("ACM") has been designated as the national authority. The ACM has various supervisory powers and can conduct independent investigations, but ultimately reports to the Commission. Only the Commission can then initiate an enforcement procedure.

Considerations for IT risk professionals and auditors

No considerations identified

Consideration for implementation (NL)

The Dutch implementation of the DMA is established through the Uitvoeringswet Digitale Markten Verordening (UDMV). This law provides the legal framework necessary to enforce the rules of the DMA in the Netherlands. It defines the responsibilities of oversight bodies and ensures the effective supervision of large online platforms, known as "gatekeepers." The UDMV grants Dutch authorities, such as the Autoriteit Consument & Markt (ACM), the power to monitor and enforce compliance with the DMA's obligations. This includes ensuring fair competition, promoting interoperability, and preventing gatekeepers from engaging in unfair business practices, such as self-preferencing their own services.

Interfaces with other legislation

None

CSRD
Corporate Sustainability Reporting Directive (Directive, 2022/2464)

Source
http://data.europa.eu/eli/dir/2022/2464/oj

Target group

The CSRD regulation applies to different categories of companies, namely (a) large companies and large groups, (b) medium-sized or small listed companies, and (c) certain non-EU companies.
(a) A large company according to the CSRD is briefly defined as a company that meets at least two of the following three criteria on two consecutive balance sheet dates:
A balance sheet total of more than € 20,000,000;
A net turnover of more than € 40,000,000; and/or
An average workforce of more than 250 on an annual basis.
A large group includes a parent company and one or more subsidiaries over which the parent has control, and where the group as a whole meets at least two of the three criteria mentioned above on two consecutive balance sheet dates.
(b) Medium-sized or small listed companies under the CSRD are companies whose securities (such as shares and bonds) are traded on a European stock exchange and which are larger than micro-enterprises. Micro-enterprises meet at least two of the following three criteria:
A balance sheet total equal to or less than € 350,000;
A net turnover equal to or less than € 700,000; and/or
An average workforce equal to or less than 10 on an annual basis.
(c) The CSRD rules apply to companies established under or governed by the law of an EU member state. An attempt has been made to also (indirectly) include companies established under or governed by the law of a non-EU member state under the CSRD under certain circumstances. This applies if there is a subsidiary or branch within the EU and/or specific turnover requirements are met.
Companies from third countries with significant activities on EU territory are required to publish a sustainability report, either directly or through their EU subsidiary or branch, particularly on the effects of their activities on social and environmental issues. Although there are some exemptions for the content of the sustainability report, such companies from third countries are thus also held accountable for their impact on people and the environment.

Applicable from

Entered into force on January 5, 2023. Applicable to large public-interest organizations (banks, insurers, listed companies) for financial years starting on or after: January 1, 2024.
Applicable to large companies and groups for financial years starting on or after: January 1, 2025.
Applicable to medium-sized or small listed companies and groups for financial years starting on or after: January 1, 2026.
Applicable to certain non-EU companies, medium-sized or small listed companies and groups for financial years starting on or after: January 1, 2028.
The first sustainability report prepared in accordance with CSRD must be published in the calendar year following the year of application.

Impact

Companies falling within the scope of application are required to report on their sustainability performance. Sustainability reporting is one of the cornerstones of the European Green Deal and the Sustainable Finance Agenda and is part of a broader policy of the European Union to require companies to respect human rights and reduce their impact on the planet. The main goal of this legislation is to enable investors and consumers to make informed sustainable choices.
The CSRD (Corporate Sustainability Reporting Directive) specifies in detail what information must be included in a company's report. The report must distinguish between short-, medium- and long-term aspects. Important elements that must be described include the business model and strategy, with attention to resilience and opportunities in the area of sustainability. Furthermore, future and investment plans must be presented, aimed at compatibility with a sustainable economy and the Paris Climate Agreement.
Other requirements include mentioning time-bound sustainability goals, their progress and scientific basis. The role of governing bodies with regard to sustainability issues, their expertise and any incentive schemes must be highlighted, along with the company's sustainability policy and applied due diligence procedures. Negative effects of own activities and the chain must be described, including measures taken and results. For cloud service providers, this is important due to the nature of their activities. They consume significant amounts of energy due to the constant operation of data centers needed to support the services, especially when (also) using artificial intelligence. Key risks related to sustainability and control measures, as well as relevant indicators, must also be reported. Companies must also declare how they have collected the necessary information in all these areas to comply with the CSRD. In addition, there is a mandatory 'limited assurance', where an external audit is necessary to ensure the reliability of the reported information. These measures are intended to encourage companies to take responsibility for their sustainability performance while improving the awareness and decision-making of investors and consumers.

Supervision and enforcement (NL and EU)

It is likely that the AFM (Autoriteit Financiële Markten) will supervise this Directive in the Netherlands. But it has not yet been established.

Considerations for IT risk professionals and auditors

Advisory and support services help organizations ensure adherence to GDPR obligations, such as lawful data processing, consent management, and data subject rights.

Consideration for implementation (NL)

The Dutch legislation will be amended to align with the CSRD (Corporate Sustainability Reporting Directive) through changes to existing laws such as the Wet op het financieel toezicht (Wft), the Wet toezicht accountantsorganisaties (Wta), the Wet op het accountantsberoep (Wab), the Burgerlijk Wetboek, and the Wet tuchtrechtspraak accountants (Wtra). The Dutch legislator is still required to specify the sanctions for non-compliance with sustainability reporting obligations. It is expected that, alongside financial penalties, non-compliance will result in reputational damage for companies.

Interfaces with other legislation

CSRD revolves around reporting sustainability efforts, while CSDDD focuses on actively identifying, preventing and reducing current risks in the supply chain.

DORA
Digital Operational Resilience Act (Regulation 2022/2554)

Source
http://data.europa.eu/eli/reg/2022/2554/oj

Target group
Financial institutions and companies that provide ICT services to these financial institutions. This includes, among others, banks, insurance companies, trading platforms, investment institutions and service providers in the field of crypto-assets. Moreover, DORA applies to ICT providers that provide services to financial companies, as well as to (ICT) companies that provide financial services themselves.

Applicable from
DORA entered into force on January 17, 2023 and applies from January 17, 2025.

Impact
DORA is a European regulation that aims to strengthen the financial sector in the EU, make it more resilient and manage IT risks more effectively against growing cyber threats, such as cyberattacks and data breaches.
Although the DORA regulation allows for delegated acts, i.e., further regulation in this area, the main lines are laid down in detail. DORA includes, among other things, the following content:
- Revised organization and governance: within the framework of DORA, specific governance and organizational requirements must be met with regard to monitoring ICT risks.
- Implementation of an ICT risk management framework: financial entities are required to implement an ICT risk management framework as part of their overall risk management system.
- ICT incident reporting: a specific procedure must be introduced for reporting incidents related to ICT.
- Digital operational resilience strategy: measures must be taken to prevent cyber incidents, detect them, limit the damage and ensure rapid recovery.
- Oversight of ICT risk management by third parties: in accordance with DORA, financial entities are responsible for the ICT risks of third parties, whereby they must define these risks and monitor them closely.

Supervision and enforcement (NL and EU)
The European Supervisory Authorities (ESAs), together with the relevant authorities, the ECB, and the ESRB, have mechanisms to foster the sharing of best practices between financial sectors and to address cyber vulnerabilities. The ESAs establish the necessary requirements through Regulatory Technical Standards (RTSs) and Joint Guidelines. The RTSs cover ICT and third-party risk management and incident classification. For further information, please refer to https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
The ESAs are also tasked with developing coordinated EU-wide cyber crisis exercises to strengthen the response to serious cyberattacks. Furthermore, they work together to enhance supervisory coordination, promote best practices, and address regulatory breaches. Oversight which is a light form of supervision will be executed over of critical third-party providers by selecting those third party providers that are most commonly used by the financial sector. The oversight is handled by the ESAs through a new directorate, ensuring consistent supervision across borders. The relevant critical third party providers are expected to be informed by the ESAs.
In the Netherlands, supervision is divided between De Nederlandsche Bank (DNB) and the Authority for the Financial Markets (AFM). DNB has been granted authority to enforce compliance with these

requirements. Sanctions may include fines, temporary suspension of services, or the revocation of licenses. Penalties can reach up to 1 percent of an institution's global turnover.

Considerations for IT risk professionals and auditors

For guidance for IT Risk professionals and auditors please refer to NOREA Studierapport "DORA in control": https://www.norea.nl/uploads/bfile/52ee1e0f-54ae-4157-9a43-524c746c2ff1

Consideration for implementation (NL)

No considerations identified

Interfaces with other legislation

DORA serves as a harmonizing framework across various financial sectors, focusing on the regulation of digital operational resilience. It complements other legislative measures, including NIS2, although the two differ significantly in scope and approach. DORA is more rule-based, reflecting its regulatory nature, while NIS2, as a directive, employs a principle-based approach and allows for varying national implementations. Furthermore, DORA and NIS2 address distinct topics, each covering aspects not present in the other.

CSDDD Corporate Sustainability Due Diligence Directive (Directive, 2024/1760)	Source https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024L1760&qid=1732697160876

Target group

The CSDDD applies to companies with more than 1000 employees and a global turnover of more than EUR 450 million. The CSDDD also applies to companies with a global turnover of more than EUR 80 million that generate more than EUR 22.5 million in royalties in the EU through franchise or license agreements, subject to a joint identity, business concept and uniform business methods.

Applicable from

The CSDD came into effect on July 25, 2024.
The implementation is carried out in phases with deadlines for different sizes of companies:
- More than 5000 employees and a net turnover of EUR 1,500 million must comply by July, 2027.
- More than 3000 employees and a net turnover of EUR 900 million must comply by July, 2028.
- More than 1000 employees and a net turnover of EUR 450 million must comply by July, 2029.

Impact

The proposed CSDDD (Corporate Sustainability Due Diligence Directive) requires large companies to continuously investigate both their own business activities and those of their permanent cooperation partners. In doing so, they must identify the effects of these activities on both the environment and human rights.
If the business activities of the companies have negative consequences for the environment and human rights, they are obliged to take appropriate measures to prevent, reduce and end these negative effects. There is a high chance that this will have a major impact on cloud service providers (especially if they develop, use or sell artificial intelligence).
Companies must annually monitor whether their own due diligence policy and the measures taken are effective.
In addition, they must set up a complaints procedure, allowing citizens, civil society organizations and trade unions dealing with negative effects to raise their objections.
The CSDDD includes a clause that describes in detail how companies should involve their stakeholders in a substantial way. Essentially, this requires that stakeholders be consulted for:
-Obtaining information about possible and actual negative effects.
-Preparing a preventive or corrective action plan.
-Making decisions about terminating business relationships.
-Implementing appropriate measures.
-If applicable, developing qualitative and quantitative indicators for monitoring due diligence activities.
Finally, companies are obliged to publicly communicate about their due diligence policy and the measures taken.
It is expected that the implementation of the CSDDD will have a significant impact on the operations of large companies. After the entry into force, they must continuously conduct due diligence research and take appropriate measures to prevent, reduce and end negative effects of their business operations.

Supervision and enforcement (NL and EU)

It is currently still unclear which supervisory authority in the Netherlands will be designated for the supervision and enforcement of the CSDDD.
The supervisory authority has the power to open an investigation on its own initiative or in response to substantiated objections if it has sufficient information about possible infringements by a company on national legislation resulting from a specific directive. If the authority determines that these national provisions are not being complied with, the company concerned must take corrective measures within a reasonable period. However, taking corrective measures does not preclude the imposition of administrative sanctions or the arising of legal liability in case of damage. The supervisory authorities have at least the power to demand that violations be terminated, repetition be prevented and appropriate remedial measures be taken. They can also impose fines and take interim measures to prevent serious and irreparable damage. When fines are imposed, they are based on the company's turnover. The sanctions imposed must be made public.

Considerations for IT risk professionals and auditors

No considerations identified

Consideration for implementation (NL)

The CSDDD is likely to be implemented in the Netherlands through amendments to existing laws, such as the Burgerlijk Wetboek and possibly the Wet op de Ondernemingsraden (WOR). New laws and regulations may also be introduced to effectively integrate and enforce the directive. The exact implementation is still under development.

Interfaces with other legislation

CSRD revolves around reporting sustainability efforts, while CSDDD focuses on actively identifying, preventing and reducing current risks in the supply chain.

NPLD
New Product Liability Directive (Directive, 2024/2853)

Source
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024L2853&qid=1732693848346

Target group
Manufacturers (and their importers and/or representatives) of products, including developers (and their importers and/or representatives) of digital manufacturing and software (with the exception of open source software developers).

Applicable from
The NPLD came into force on December 9, 2024. The new rules will apply to products placed on the market on December 9, 2026 (24 months after the directive came into force).

Impact
The new product liability directive includes several important changes to ensure better protection of consumers and to promote equal regulation within the EU.
The definition of a product is expanded to include software, artificial intelligence and digital services such as robots, drones and smart home systems. However, open source or free software falls outside these rules due to their reliance on user improvements, which means developers cannot be held liable.
One of the most important changes is that the burden of proof for victims in complex cases is eased, making it easier to obtain compensation. In addition, manufacturers can now be obliged to disclose evidence in case of defective products.
The revised directive also provides for compensation for medically recognized psychological harm and for the destruction or irreversible damage of data. Furthermore, the directive establishes that there must always be liability within the EU for damage caused by a defective product, even if it is manufactured outside the EU. This can make the manufacturer's authorized representative or, ultimately, the fulfillment service provider (a company that typically provides storage, packaging and shipping services) liable. If there is no liable company, consumers can still get compensation through national schemes.
All in all, the directive aims to establish consistent regulations for all Member States, with the goal of promoting a well-functioning digital and circular economy and helping victims of damaged or defective products obtain fair compensation.

Supervision and enforcement (NL and EU)
No supervisory authority is appointed for this regulation. This legislation can be used in a civil lawsuit to presume causality, thereby easing the burden of proof for victims.

Considerations for IT risk professionals and auditors

No considerations identified

Consideration for implementation (NL)

The Dutch name of the Product Liability Directive is "Aansprakelijkheids Richtlijn" (AR). The AR must be transposed into national legislation by the member states. In the Netherlands, this likely means adjustments will be made to existing laws, such as the Dutch Civil Code, to implement the new requirements and rules of the directive. Once the directive has been officially adopted, the member states will have a specific period to incorporate it into their national legal systems.

Interfaces with other legislation

None