Unified Digital Management Model

Navigating the European digital decade: Building trust and innovation through unified regulatory compliance

Version 1.0

May 2025

The better the question.
The better the answer.
The better the world works.

Shape the future with confidence

ONLINE TRUST COALITIE

Foreword

Digitalization has become an integral part of our society and is the backbone of our economy. In fact, every organization depends on its information technology. Our current day-to-day business and future innovations cannot exist without a reliable digital infrastructure. Critical parts of our society cannot operate if information technology fails — cars cannot drive, airplanes cannot fly, factories cannot produce, hospitals cannot operate, and financial markets will disrupt.

As a society, we must be in control of our digital systems and processes. That is a responsibility of everyone who operates systems that are part of this infrastructure and especially those who operate systems that are critical and vital to our society. Therefore, the European Union has implemented many regulations that safeguard the safety, trust and resilience of our digital infrastructure, the use of data and the impact on our markets. In total more than 100 regulations are in force, each dealing with specific aspects.

Organizations that play an important part in the digital infrastructure, or rely on it, experience a significant challenge. On the one hand, they must be innovative and utilize information technology to the best extend they can. On the other hand, they must ensure the utilized technology is safe, trusted, reliable and compliant towards the many regulations that are imposed. This balancing act between opportunity, risk and compliance is one that the market, especially in Europe, faces and struggles with.

Therefore, both EY and the Online Trust Coalition came together to help organizations in their efforts to comply with the requirements these regulations impose on them while staying innovative and competitive. We strongly believe that organizations that demonstrate a professional attitude towards digital control, should be able to cope with regulatory requirements imposed upon them without impacting their ability to innovate. To support organizations with this cause, we are proud to present the Unified Digital Management Model. This model translates the requirements from four important European regulations (GDPR, AI Act, NIS2 and DORA) into one set of generally accepted design principles for digital control. This will help organizations in their compliance efforts, it will reduce administrative burden and will also have a positive impact on regulatory effectiveness for the society. And as a result, it helps organizations to become resilient and secure. Our gratitude goes out to the organizations and specialists that worked together in composing this model.

About EY

EY, or Ernst & Young, is a global professional services firm that provides a range of services including assurance, tax, and consulting. EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets. Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow. EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

About the Online Trust Coalition

The Online Trust Coalition (OTC) is a public-private partnership initiated by the Dutch Ministry of Economic Affairs. This collaboration involves both public and private entities with the aim of enhancing trust in online services. The OTC endeavors to make trust more tangible—providing user organizations, supervisors, and other stakeholders with clearer and better interpretable information on the security and resilience of systems and services. For providers, the OTC offers a cost-effective and less disruptive method to demonstrate their trustworthiness. Their current focus is on streamlining compliance processes and enhancing the effectiveness of regulations.

Disclaimer

This Unified Digital Management Model is based on the following regulatory documents:

GDPR:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

DORA:

- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 23 February 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act).

NIS2:

- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

AI Act:

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

In the event of changes to any of the aforementioned documents made after May 2025, these will be incorporated into the next publication of the Unified Digital Management Model. Any changes in such content will be promptly communicated.

The Unified Digital Management Model should not be used to demonstrate compliance with any of the aforementioned legislations. Instead, it is intended as a tool to support the management of regulatory requirements related to digital trust in a more systematic and proactive manner. It supports in enhancing the maturity of specific organizational processes and encourages collaboration and lineage among people, processes, and technology to increase efficiency and manage compliance costs.

Building on this, the design principles included in the Unified Digital Management Model do not encompass all regulatory requirements from the aforementioned legislations. The purpose of implementing this unified set of design principles is to enable organizations to meet the majority of requirements across all relevant regulations in a unified and simplified manner. A corresponding Statement of Applicability will provide insight into the related articles that informed the definition of the design principles. This Statement of Applicability is a separate document and not included in this document.

Lastly, industry best practice documentation has been used as input to establish the accompanying implementation guidance.

Intellectual property rights

Contents

Introduction to the Unified Digital Management Model

1. Introduction to the Unified Digital Management Model

1.1. Evolving digital regulatory frameworks

In recent years, the rapid adoption of multiple technologies has reshaped the landscape of business and society. Organizations are increasingly leveraging advancements in artificial intelligence (AI), cloud computing, and data analytics to drive innovation and create new products and services. This swift integration of technology not only enhances operational efficiency but also transforms customer experiences, enabling organizations to respond more effectively to market demands.

However, as organizations embrace these technological advancements, concerns regarding the responsible, trustworthy, and secure use of these innovations have grown significantly. Stakeholders are increasingly aware of the potential risks associated with data privacy, cybersecurity, and ethical considerations in technology deployment. Citizens are demanding greater transparency and accountability from organizations, seeking assurance that their personal information is handled with care and integrity.

The competitive positioning of big tech companies further complicates this landscape. Their dominance in the digital market raises questions about fairness and equity, as smaller organizations struggle to compete on the same level. This concentration of power not only impacts market dynamics but also heightens the risks associated with technological dependence. As businesses become more reliant on digital infrastructure, the potential for operational disruptions increases, exposing them to vulnerabilities that can have far-reaching consequences.

In response to these challenges, the European Commission has announced the Digital Decade, a comprehensive legislative agenda aimed at enhancing oversight and regulation of digital practices across Europe. This initiative seeks to establish a robust framework that addresses the pressing need for accountability in the digital space, ensuring that organizations can navigate the complexities of digital regulation effectively.

The Digital Decade leads to the introduction of more laws and regulations governing digital practices, fostering an environment where trust and resilience are at the center. By implementing these measures, the European Commission aims to create a secure digital ecosystem that not only protects individual rights but also promotes responsible usage of technology in business processes.

As we move forward in this evolving digital landscape, it is crucial for organizations to understand how to create trust in their digital assets, ensuring resilience while promoting responsible usage. The Unified Digital Management Model will play a vital role in this context, providing a structured approach to managing digital regulatory requirements and enabling organizations to comply with existing regulations while anticipating future challenges.

The digital decade

The European Commission seeks to accelerate the digital transformation of businesses and public services, secure sustainable Digital Assets and increase digital capabilities across the European Union (EU).

Together these objectives and drivers have led to the need for new regulations and directives on a wide array of topics relating to technology, digital capabilities and the digital economy.

1.2. Understanding related challenges

While the goals of the Digital Decade are admirable, the avalanche of new regulation is causing issues for many organizations. And while each new law may be looking at the digital world from a specific angle (security, privacy, data access) they all affect how organizations process data, develop systems and further digitize their business. This jungle of new legislation is making it harder for organizations to operate cost effectively and innovate.

Furthermore, the current geopolitical developments require the EU to rethink its position compared to major players in the US and China. While both these regions prioritize innovation and technological advancement, the EU often gets caught up in regulations that can limit its competitiveness. As the US and China race ahead in technological capabilities, the EU must strike a balance between necessary regulation and fostering an environment that encourages innovation, ensuring that it does not fall behind in the global digital landscape.

In short, the following issues can be identified:

Increased control burden could slow down innovation:

New regulations introduced as part of the European Digital Decade mandate additional controls and compliance measures. While the regulations are designed to enhance data security and operational resilience, they also impose a significant burden on organizations. The increased focus on regulatory compliance can divert resources and attention away from innovation, stifling the development of new technologies and digital solutions. Organizations may find themselves spending more time and effort on meeting regulatory requirements rather than on creative and strategic initiatives.

Unleveled playing field increases the risk of forum shopping:

The diverse regulatory environment within the EU can create an uneven playing field for businesses. Organizations might engage in "forum shopping," choosing to operate in member states with less stringent regulations to minimize compliance costs and operational difficulties. This practice can undermine the overall goals of the European Digital Decade, as it leads to inconsistencies in digital transformation efforts across the EU. A more harmonized regulatory approach is essential to ensure fair competition and uniform progress in achieving digital transformation objectives.

Lack of harmonization increases complexity and compliance risk:

The European Digital Decade aims to unify digital regulations across member states, but the lack of harmonization across these regulations can lead to inconsistencies. These discrepancies make it challenging for organizations to comply uniformly, increasing compliance risks and operational complexities. As the regulatory landscape becomes more fragmented, businesses find it harder to navigate and implement compliant digital practices across different jurisdictions.

Lack of mapping with existing industry standards increases the risk of inefficient implementation:

The European Commission's ambitious digital transformation goals require alignment with existing industry standards. However, the absence of clear mappings to these standards can lead organizations to adopt inefficient implementation strategies. Without a standardized approach, businesses risk redundant efforts and increased costs, ultimately slowing down their ability to innovate and adapt to new regulations such as the Digital Operational Resilience Act and the Digital Services Act.

1.3. Call to action

In summary:

1. A wave of European regulation is emerging to guide how we **use, trust** and protect digital assets.
2. While these regulations may cover different topics, they often involve **similar stakeholders** and digital assets.
3. Therefore, we advise shifting from a **regulation-by-regulation perspective** to a **unified domain perspective**, enabling organizations to navigate the complexities of the digital landscape more effectively. In this way, implementing requirements from individual legislations are no one-off exercises anymore, but small building blocks that are incorporated into a strong unified fundament.
4. This unified approach not only **simplifies** the compliance process but also enables organizations to leverage synergies between regulations, ultimately enhancing their operational efficiency and innovation capacity.

Towards a unified approach

2. Towards a unified approach

2.1. The purpose of implementing a unified approach

As described in the previous chapter, organizations are struggling with an increase in (unharmonized) European Regulations. So how are organizations dealing with these regulations? Traditionally, organization often **tackled each regulation individually**, launching specific projects dedicated to meeting the distinct requirements of each law. However, this is not an effective approach as it leads to potential duplication, organizational complexity, and blind spots.

Refer to the following section for more details how organizations now struggle in their regulation-by-regulation approach:

1. Potential duplication due to overlap

Many of these **regulations share common elements**. For example, all regulations require a level of governance and risk management, and privacy cannot be achieved without security measures. Adopting a regulation-by-regulation approach can lead to redundancy and inefficiency, as it often results in duplicated efforts in addressing similar processes and topics from slightly varied perspectives.

The following table provides illustrative examples of common areas where regulatory requirements typically overlap, highlighting the need for a more integrated approach to governance and compliance.

Examples of shared or common elements

Management body versus Management

- DORA and NIS2 place active responsibility for security with the "Management body", as in the highest level in the organization. While other regulation do not prescribe this or use more generic terms such as "Management". In a unified approach we ensure that we use a similar understanding of the organization and ensure responsibilities are assigned at the right level from the start (instead of a pick-and-mix).

Incident management

- Reporting incidents to various regulators is a common requirement across many European regulations. Each regulation may specify different reporting periods and necessitate communication with distinct regulatory bodies. Traditionally, organizations might prepare separate overviews for each regulation, addressing the requirements in isolation. However, by adopting a unified approach, organizations can streamline these processes, creating a unified overview that integrates all the regulatory requirements into one comprehensive framework.

Data models & inventories

- Regulations such as DORA, GDPR, and the AI Act mandate that organizations maintain specific inventories or overviews (e.g., concerning AI-systems, critical functions, or processing activities). Although each regulation requests information from its unique perspective, it is essential to compile this data centrally within the organization. Creating these overviews independently risks duplicative effort and the establishment of registers that may not be regularly updated. Adopting a unified approach involves creating a unified data model to consolidate and manage this information efficiently.

2. Siloed approach leading to organizational complexity

Defining a new governance structure, including roles and responsibilities, for each law can significantly increase organizational complexity. If each new regulation necessitates a distinct governance framework, it will lead to potential overlaps, redundancies, and the burden of managing multiple concurrent structures. This can strain resources. Furthermore, presenting the business with specific requirements for every individual law can be overwhelming. The constant influx of new and unique compliance demands may lead to confusion, resistance, and difficulty in prioritizing efforts. This fragmentation can divert focus from core business activities, negatively impacting overall productivity and morale.

3. Digital trust is not achieved with just one discipline

To build digital trust, consumers expect both security and privacy, as well as ethical behavior from organizations in handling their data. It is important to recognize that these are not just singular components but integral expectations of consumers. Adopting a regulation-by-regulation approach may result in an overemphasis on one aspect, thereby creating potential blind spots.

2.2. Towards a unified approach

Therefore, a unified approach is proposed to help. A unified approach to compliance entails an integrated strategy that aligns various regulatory requirements to create a streamlined process, reducing redundancy and enhancing efficiency.

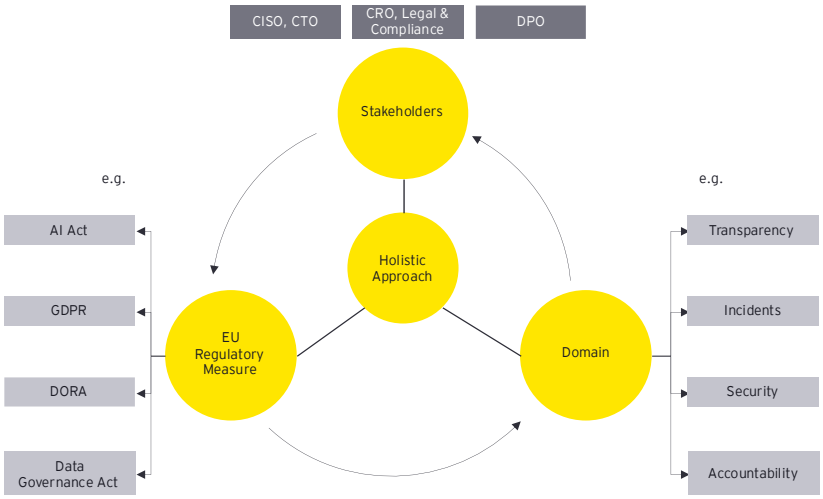


Figure 1: Reflecting a unified approach

- **Defining common building blocks instead of a regulation-by-regulation approach.** Building a common set of capabilities across regulations to build a good basis. Additionally, identifying overlaps between different regulations is crucial. This includes mapping regulatory requirements, assessing risks, and designing integrated compliance programs that address multiple regulations simultaneously. This involves standardizing policies and practices, establishing centralized management systems, and fostering collaboration to develop common guidelines.
  - The Unified Digital Management Model is designed to provide a model that can be applied across different regulatory environments. It includes key elements such as data privacy standards, cybersecurity measures, and risk management protocols. By incorporating these shared components, the model helps streamline regulatory processes and ensure consistency in implementation. Additionally, it offers flexibility to adapt to specific regional or industry-specific rules, making it a versatile tool for regulatory management.
  - In the next chapter, detailed information about the development process of the Unified Digital Management Model. This section will also cover the benefits of using the model, such as improved efficiency, reduced duplication of efforts, and enhanced transparency in regulatory compliance.

- **Cross-functional collaboration.** For a true unified approach, we cannot just rely on a model or on a framework, we will also need to incorporate this in our ways of working. A unified approach prescribes not only the implementation of common domains, but also the cross-functional collaboration between domains. If we recognize that trust of consumers is not just based on security or privacy, but on a combination of factors, we need to also organize ourselves in that manner.
  - **Rethinking operating models.** Implementing the unified approach within organizations goes beyond implementing a framework with design principles; it necessitates a new approach to managing regulatory compliance, resulting in changes to the organization's Target Operating Models. This shift emphasizes stronger multidisciplinary collaboration and the integration and lineage of the organization's Policy House, which have grown increasingly complex over time.
- **Complete the Plan-Do-Check-Act (PDCA) cycle.** Next to setting a common guideline (plan) we also need to ensure we complete the Plan-Do-Check & Act steps together. This involves implementing continuous monitoring mechanisms ensuring ongoing compliance and adaptability to regulatory changes. This includes monitoring for new regulations affecting how the organization can utilize digital assets, data or infrastructure. In a unified approach we also want to streamline reporting lines to ensure all domains have an appropriate reporting body or platform.
  - **Technology** can support in helping organizations incorporate a PDCA cycle. In a unified approach we should avoid having too many different tools & technologies utilized for across domains and stakeholder groups (e.g., to register incidents, risks or controls).

Adopting a unified approach to regulatory compliance offers numerous advantages, particularly in establishing a proactive management system. This approach involves comprehensive governance practices that can be seamlessly adapted to accommodate emerging technologies and regulations such as quantum computing, data sovereignty, or cloud solutions.

2.3. Benefits of a unified approach

Benefits of a unified approach include:

- **Controlled compliance costs reduction:** A unified approach simplifies compliance processes by identifying overlapping regulatory requirements, thus reducing redundant efforts and lowering overall compliance costs. By streamlining these processes, organizations can allocate resources more efficiently and achieve cost savings.
- **Decreased risk of non-compliance:** By adopting a unified approach, organizations can ensure that all regulatory requirements are met comprehensively. The integrated framework allows for continuous monitoring and updating of compliance measures, thereby reducing the risk of non-compliance and potential legal penalties.
- **Cross-functional collaboration:** The implementation of a unified approach fosters collaboration across various departments within an organization. By aligning compliance efforts with business goals, different teams can work together more effectively, sharing insights and expertise to achieve a unified compliance strategy.
- **More time for higher-value activities:** With streamlined compliance processes and reduced complexity, organizations can allocate more time and resources to higher-value activities. This enables them to focus on strategic initiatives, innovation, and overall business growth, rather than being bogged down by compliance-related tasks.

In the following chapter the Unified Digital Management Model is further fleshed out describing how to build a common model.

Building the Unified Digital Management Model

3. Building the Unified Digital Management Model

3.1. Components of the Unified Digital Management Model

The Unified Digital Management Model is a concept designed to address common or shared requirements in the realm of digital trust. This model aims to provide structure and guidance to assist organizations in adopting regulation in a repeatable and efficient manner. The model is generic, ensuring their applicability across multiple regulations. They outline what organizations should do, while the corresponding implementation guidance provides support on how to achieve this.

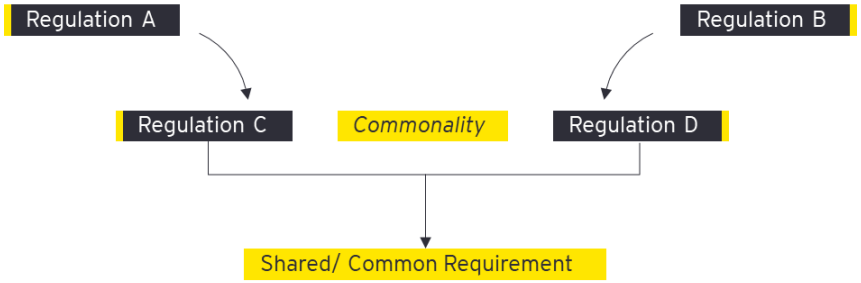


Figure 2: From regulation-based to domain-based

- A first step towards a unified approach is to identify the **common domains, or themes** originating from requirements of the various regulations (refer to figure 1). For instance, the reporting of incidents to regulators or government institutions is a theme occurring in various regulations.
- For each identified theme **design principles (the "What")** are formulated that serve as objectives for organizations to achieve. For the definition of these design principles, common requirements are being extracted from individual regulations, as illustrated in Figure 2. These principles are generic in nature, ensuring their applicability across multiple regulations.
- To provide more tangible and concrete guidance, **implementation guidance (the "How")** is defined. The implementation guidance supports organizations in adhering to and enacting these design principles. This implementation guidance includes concrete actions that organizations can take to effectively implement the design principles.

3.2. Scoping by using a phased approach

As indicated, the primary objective of this unified approach is to identify overlaps and efficiencies across various themes, enabling organizations to streamline their compliance efforts and enhance their digital practices. The model is developed through a phased approach, starting with a limited set of regulations in Phase 1, with the intention of further expanding the model by incorporating additional laws and regulations in Phase 2. The Unified Digital Management Model, which includes the legislation from Phase 1 as outlined below, is now released in the second quarter of 2025, while Phase 2 is planned for release in 2026.

Phase 1 (current): GDPR, NIS2, DORA, AI Act

General Data Protection Regulation (GDPR)	Network & Information Systems Security Directive (NIS2)	Digital Operational Resilience Act (DORA)	Artificial Intelligence Act (AI Act)

Phase 1 is centered around critical digital legislation that is currently in effect, specifically the General Data Protection Regulation (GDPR), the Network & Information Systems Security Directive (NIS2), the Digital Operational Resilience Act (DORA) and the Artificial Intelligence (AI) Act. These regulations

represent essential components of the EU's digital landscape and provide foundational requirements for organizations operating within this jurisdiction.

The requirements of this initial set of legislation have been translated into the current design principles. The Unified Digital Management Model will be subject to an annual review to anticipate regulatory changes. Subsequent phases will focus on analyzing the existing design principles to determine whether any should be added or adjusted. The model will be built over time, ultimately encompassing a comprehensive set of European digital legislation.

Phase 2 (future): DA, DGA, CRA & others

Phase 2 will extend the framework to encompass additional legislation, including the Data Act, the Data Governance Act and the Cyber Resilience Act. This phase aims to prepare organizations for new or upcoming regulatory changes by providing guidance on (anticipated) requirements, thereby enabling them to proactively adapt their digital strategies and ensure compliance.

3.3. How organizations can use the Unified Digital Management Model

The implementation of the Unified Digital Management Model provides organizations with a systematic approach for integration into their PDCA cycle. It enables organizations to adapt efficiently and quickly to new developments in the digital space, such as emerging legislation. While implementing the Unified Digital Management Model does not automatically ensure compliance with relevant legislation, it delivers an integrated, efficient, and targeted system for managing an organization's digital practices. This model simplifies navigation through the complex EU regulatory landscape and frees up valuable time and resources, allowing organizations to focus on higher-value activities, such as innovation.

The design principles within the Unified Digital Management Model do not cover all regulatory requirements from the relevant legislations. Their primary purpose is to empower organizations to address the majority of requirements across various legislations in a unified and simplified manner. However, it is essential to recognize that individual legislations will always have specific requirements that must be followed. A corresponding Statement of Applicability will provide valuable insights into how the model aligns with specific regulatory obligations.

Furthermore, the Unified Digital Management Model can be utilized by organizations in multiple ways:

- **Framework for compliance:** Use the model as a foundational framework to understand and navigate the complexities of regulatory requirements. It provides a structured approach to identifying what needs to be done to comply with various regulations, making it easier for organizations to align their practices accordingly.
- **Risk assessment tool:** Utilize the model to conduct risk assessments related to data management and compliance. By identifying potential vulnerabilities and areas of non-compliance, organizations can prioritize their efforts and allocate resources effectively to mitigate risks.
- **Benchmarking and best practices:** Organizations can use the model to benchmark their current practices against the Unified Digital Management Model. This comparison can highlight areas for improvement and inspire the adoption of innovative solutions to enhance digital trust.
- **Collaboration with stakeholders:** Engage with clients, suppliers, and other stakeholders using the model as a common reference point. This collaboration can facilitate discussions around digital trust, compliance expectations, and shared responsibilities in managing sensitive data.
- **Reporting and accountability:** Use the model to establish reporting mechanisms that ensure transparency and accountability in digital trust efforts. Regularly report on compliance status,

risk management activities, and progress toward achieving digital trust objectives to stakeholders.

- **Adaptation to changing regulations:** As regulations evolve, organizations can use the model as a flexible tool to adapt their practices accordingly. The model's generic nature allows organizations to apply it to various regulatory frameworks, ensuring ongoing compliance in a dynamic environment.

3.4. Relevant audience

Managing digital trust by organizations is not only of interest to clients, employees, and suppliers, but it is also crucial for all stakeholders. Both internally and externally The Unified Digital Management Model is designed to be relevant for a diverse range of stakeholders involved in the realm of digital trust and regulatory compliance. Key audiences include:

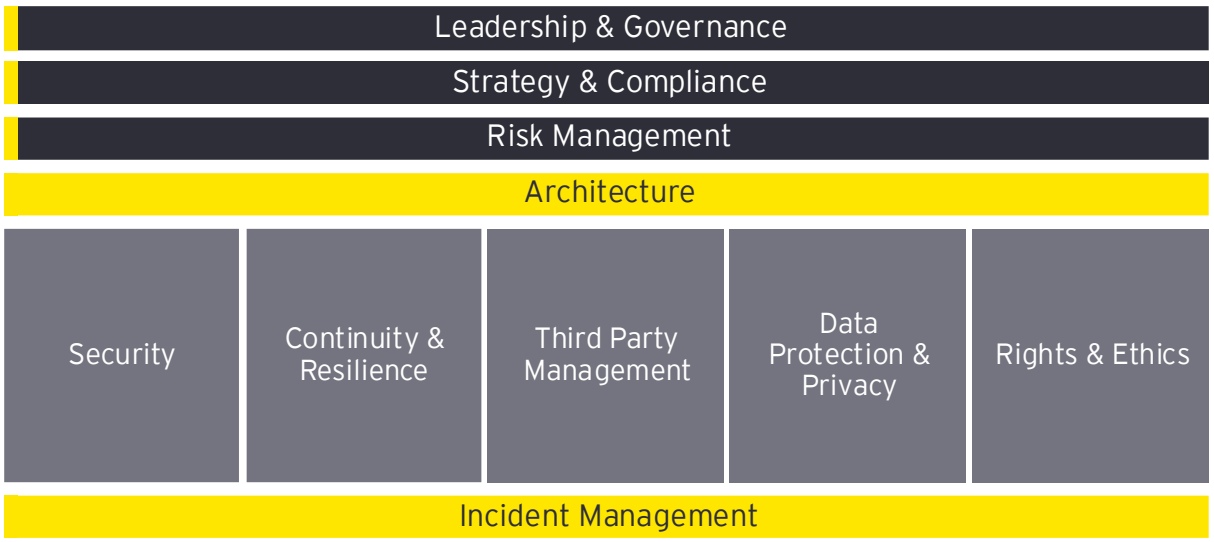
- **Organizations across industries**: Businesses of all sizes and sectors, including finance, healthcare, technology, and retail, can benefit from the model. It provides a structured approach to understanding and implementing regulatory requirements related to data privacy, security, and trust.
- **Board members and executives:** Members of the board and executive leadership teams play a crucial role in setting the strategic direction of organizations. The Unified Digital Management Model provides them with insights into regulatory compliance and digital trust, enabling informed decision-making and risk management at the highest levels. It empowers them to foster a culture of compliance and trust within the organization, ensuring that digital trust is prioritized as a core business objective.
- **Compliance officers and legal teams:** Professionals responsible for ensuring that organizations adhere to regulations will find the model invaluable. It offers clear guidelines on what needs to be done to comply with various regulations, making their job more manageable.
- **Data governance and risk management teams:** Teams focused on data governance and risk management can leverage the model to identify shared requirements and best practices. This will help them develop strategies that enhance data protection and mitigate risks associated with non-compliance.
- **IT- and security professionals:** Information technology and cybersecurity teams can use the model to align their technical implementations with regulatory expectations. It provides insights into the necessary controls and measures to establish a secure and trustworthy digital environment.
- **Clients:** Clients of organizations are increasingly concerned about how their data is managed and protected. The Unified Digital Management Model helps organizations demonstrate their commitment to digital trust, ensuring clients feel secure in their interactions and transactions.
- **Suppliers:** Suppliers play a critical role in the supply chain and are often exposed to sensitive data. The Unified Digital Management Model provides guidance on how organizations can manage digital trust with their suppliers, fostering secure partnerships and compliance throughout the supply chain.
- **Regulatory bodies and policymakers:** Entities involved in shaping regulations can use the model to understand common challenges faced by organizations. This insight can inform the development of clearer and more effective regulatory frameworks.

By addressing the needs of these diverse stakeholders, the Unified Digital Management Model aims to foster a collaborative approach to achieving digital trust and regulatory compliance across organizations.

The Unified Digital Management Model Standard

4. The Unified Digital Management Model

The Unified Digital Management Model is organized around ten key themes. Some of these themes are overarching and influence the entire organization, such as Leadership & governance, while others pertain to specific organizational processes, such as Security. The graphic below illustrates the coherence between the different type of themes.



The structure of the Unified Digital Management Model across the ten key themes are as follows:

- Foundational themes:

  These themes serve as the foundational pillars of the organization, guiding its overall direction and ensuring alignment with regulatory requirements. They encompass critical areas which collectively shape the organization's compliance culture and strategic objectives. The following themes are classified as foundational themes:

  - Leadership & governance
  - Strategy & compliance
  - Risk management

- Transversal processes:

  These themes focus on processes that span across the organization and support various capabilities. Transversal Processes refer to the organizational processes that are not confined to a single department or function but instead span across multiple areas of the organization. These processes are essential for ensuring that various capabilities work together effectively to support the overall objectives of the organization. The following themes are classified as transversal processes:

  - Architecture
  - Incident management

- Topic-based pillars

  These themes outline the minimum expectations for specific topics or capabilities. The following themes are classified as topic-based pillars:

  - Security
  - Continuity & resilience
  - Third-party management
  - Data protection & privacy
  - Rights & ethics

The ten themes are translated into 36 sub-themes for which design principles are defined. A design principle in the Unified Digital Management Model is a basic guideline that helps organizations manage digital trust and follow regulations. These principles provide a clear way for organizations to set up rules, policies, and practices that ensure they are responsible, transparent, and able to manage risks effectively. They help organizations deal with complex regulations by encouraging best practices and aligning their operations with both their goals and the requirements of the outside world. These principles focus on being flexible, complete, and adaptable, allowing organizations to respond quickly to new laws and changes in the digital landscape.

The table below provides an overview of the sub-themes part of the Unified Digital Management Model.

#	Theme	#	Sub-Theme
1	**Leadership & Governance**	1.1	Accountability and Oversight
		1.2	Governance Policies & Procedures
		1.3	Training & Awareness
2	**Compliance**	2.1	Conformity Assessment & Periodically monitoring
		2.2	Authority Cooperation
3	**Risk Management**	3.1	Risk Governance
		3.2	Risk Identification
		3.3	Risk Assessment
		3.4	Risk Response
		3.5	Risk Reporting and Monitoring
		3.6	Control Frameworks
4	**Architecture**	4.1	Formalizing the Business Architecture (Functions, Processes)
		4.2	Identifying IT Assets and Systems
5	**Security**	5.1	Organizational Controls
		5.2	Technical Security
		5.3	People Controls
		5.4	Physical Controls
6	**Continuity & Resilience**	6.1	Resilience Governance & Oversight
		6.2	Minimal Viable Organization
		6.3	Resilience strategy & planning
		6.4	Resilience capabilities
		6.5	Resilience monitoring & Assessment
7	**Third Party Management**	7.1	Third Party Management Governance and Oversight
		7.2	Third Party Management Policy & Procedures
		7.3	Third Party Management Lifecycle

#	Theme	#	Sub-Theme
		7.4	Third Party Management Reporting
8	**Data Protection & Privacy**	8.1	Data protection & privacy principles
		8.2	Data Sharing
		8.3	Privacy by Design
9	**Rights & Ethics**	9.1	Ethical oversight
		9.2	Complaints and Requests
		9.3	Informed consent & Transparency
10	**Incident Management**	10.1	Incident Identification & Classification
		10.2	Incident Response
		10.3	Incident Notification & Reporting
		10.4	Post Incident & Lessons Learned

The remaining sections of this document, divided across ten themes, are structured in a consistent manner. Each section addresses a specific theme, which is developed as follows:

- **Definition of the theme:** An explanation of the main theme being discussed.
- **Related sub-themes:** Identification of sub-themes that fall under the main theme.
- **Definition of the sub-theme:** A clear definition of each sub-theme.
- **Design principle:** The core principle related to the sub-theme.
- **Implementation guidance:** Practical guidance on how to implement the design principle.
- **Mapping to related articles:** References to the articles that provided input for the design principle.

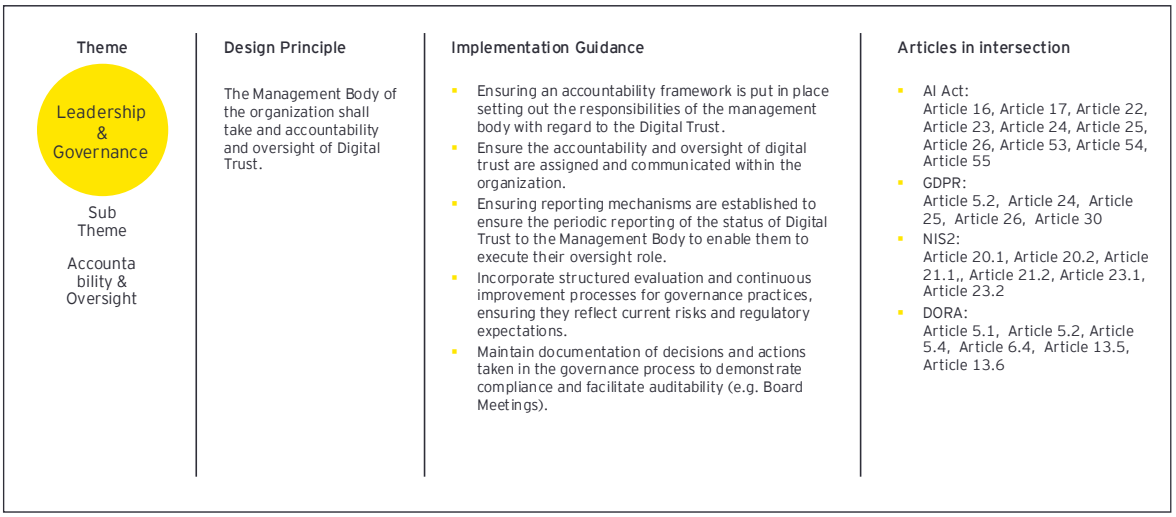


Figure 3: Example of the Unified Approach

Statement of Applicability (SoA)

Next to this Standard, the Statement of Applicability (SoA) serves as a crucial document. It provides an overview of the regulatory (sub)articles that have informed the development of the design principles. It includes a mapping per (sub)article of the regulatory articles with the relevant design principles. The detailed Statement of Applicability can be freely requested by contacting the authors or emailing rudrani.djwalapersad@nl.ey.com.

Articles that are related to scope or definitions are deemed out of scope. Furthermore, the following exclusions have been made in the SoA, to account for regulatory articles that are only applicable to regulatory authorities or very specific organizations:

- Under the GDPR, the focus is exclusively on the articles that apply to Controllers, Joint Controllers, and Processors, as well as to Data Protection Officers. Provisions related to Supervisory Authorities, the European Data Protection Board, and other entities are considered out of scope.
- Similarly, in the context of the AI Act, the scope is limited to the responsibilities of Providers, Deployers, Importers and Distributors, deliberately omitting requirements for various oversight authorities that fall outside this model.
- For DORA, the concentration is on the obligations relevant to Financial Entities, excluding requirements that pertain to ESAs, Central Securities Depositories, and other supervisory bodies.
- Lastly, articles from NIS2 that emphasize considerations for Essential and Important Entities are included in scope, while those that apply to Member States or CSIRTs are excluded.

4.1. Leadership & governance

Theme definition: Leadership refers to defining the strategic direction, crafting a clear vision and objectives, and promoting accountability throughout the organization. Governance refers to the frameworks, roles & responsibilities, policies, and processes established to guide, control, and manage the operations and strategies of an organization.

Sub-themes:

- Accountability & oversight
- Governance policies & procedures
- Training & awareness

4.1.1. Sub-theme: Accountability & oversight

Sub-theme definition: Accountability and oversight refer to the mechanisms and processes through which individuals and organizations are held responsible for their actions and decisions, ensuring transparency and adherence to established standards and policies. This involves monitoring, evaluating, and reporting on performance and compliance to maintain integrity and trust within the organization and among stakeholders.

Design principle: 1.1 Accountability & oversight			
Theme	Leadership & governance	**Sub-theme**	Accountability & oversight
Design principle	The management body of the organization shall be assigned with accountability and oversight responsibilities for digital trust, ensuring they uphold and enforce digital trust principles and practices.		

Design principle: 1.1 Accountability & oversight			
Implementation guidance	▪ Development and implementation of an accountability framework that clearly defines the responsibilities of the management body and all staff regarding the organization's digital trust practices. ▪ Ensuring that the roles and responsibilities for accountability and oversight of digital trust are clearly assigned and communicated throughout the organization. ▪ Establishment of robust reporting mechanisms to ensure the accountability and oversight of the management body. Embed these mechanisms across all levels of the organization to promote transparency and compliance. ▪ Integration of structured evaluation and continuous improvement processes into governance practices. Regularly review and update these processes to reflect current risks and regulatory expectations. ▪ Maintenance of documentation of decisions and actions taken in the governance process. This documentation should demonstrate compliance and facilitate auditability, ensuring a record of governance activities.		
Article mapping			
AI ACT Ref#	▪ Article 16 ▪ Article 17 ▪ Article 22 ▪ Article 23 ▪ Article 24 ▪ Article 25 ▪ Article 26 ▪ Article 53 ▪ Article 54 ▪ Article 55	**GDPR Ref#**	▪ Article 5 ▪ Article 5.2 ▪ Article 24 ▪ Article 25 ▪ Article 26 ▪ Article 30
NIS2 Ref#	▪ Article 20.1 ▪ Article 20.2 ▪ Article 21.1 ▪ Article 21.2 ▪ Article 23.1 ▪ Article 23.2	**DORA Ref#**	▪ Article 5.1 ▪ Article 5.2 ▪ Article 5.4 ▪ Article 6.4 ▪ Article 13.5 ▪ Article 13.6

4.1.2. Sub-theme: Governance policies & procedures

Sub-theme definition: Governance policies and procedures are the formal guidelines and processes established by an organization to ensure effective decision-making, accountability, and compliance with legal and regulatory requirements. They provide a structured framework for managing the organization's operations, mitigating risks, and achieving strategic objectives while maintaining transparency and integrity.

Design principle: 1.2 Governance policies & procedures			
Theme	Leadership & governance	**Sub-theme**	Governance policies & procedures
Design principle	The management body shall define, approve, oversee, and be responsible for the implementation of all arrangements related to the organization's digital trust framework, ensuring alignment with strategic objectives and maintaining accountability and transparency.		
Implementation guidance	▪ Development and implementation of policies and procedures as part of the digital trust framework to ensure robust governance and compliance. ▪ Formulate digital trust policies and objectives that align with the organization's overarching strategic aims, ensuring coherence and support for the organization's mission. ▪ Ensuring that organizational processes are adjusted and aligned with the requirements of the digital trust management system to maintain consistency and effectiveness. ▪ Allocation of the necessary assets and support to effectively implement and maintain the digital trust management system, ensuring it has the resources needed to function properly. ▪ Ensuring sufficient communication about the digital trust management system throughout the organization to promote awareness and understanding among all staff. ▪ Ensuring that the digital trust management system is effectively fulfilling its intended purposes and achieving its goals. ▪ Promotion and ensuring of sufficient contribution from individuals to enhance the effectiveness of the digital trust management system, fostering a culture of accountability and participation. ▪ Implementation of processes to facilitate the continual improvement of the digital trust management system, regularly reviewing and updating practices to address emerging risks and opportunities. ▪ Assisting key management personnel in demonstrating their leadership in relation to their specific duties, ensuring they actively support and promote the digital trust management system within their areas of responsibility.		
Article mapping			
AI ACT Ref#	▪ Article 9.1 ▪ Article 9.2 ▪ Article 10.1 ▪ Article 17	**GDPR Ref#**	▪ Article 5.2 ▪ Article 6 ▪ Article 24.1 ▪ Article 24.2 ▪ Article 25.1 ▪ Article 25.2 ▪ Article 28.1 ▪ Article 32.1 ▪ Article 35.7

Design principle: 1.2 Governance policies & procedures			
NIS2 Ref#	▪ Article 21	**DORA Ref#**	▪ Article 5.1 ▪ Article 5.2

4.1.3. Sub-theme: Training & awareness

Sub-theme definition: Training and awareness programs educate staff about their roles and responsibilities in areas such as compliance, resilience, privacy, and security, ensuring they handle organizational tasks competently and informedly. These programs aim to enhance employees' knowledge and skills, promoting adherence to organizational standards and regulatory requirements.

Design principle: 1.3 Training & awareness			
Theme	Leadership & governance	**Sub-theme**	Training & awareness
Design principle	Organizations shall establish, implement, and maintain continuous training and awareness programs on digital trust topics for all staff, including the management body, to ensure comprehensive understanding and adherence to digital trust principles across the organization.		
Implementation guidance	▪ Conducting a thorough assessment to identify the specific digital trust training needs of the organization, considering roles (incl. management body), responsibilities, regulatory requirements, and knowledge gaps. ▪ Development and implementation of a comprehensive training plan that outlines objectives, content, delivery methods, and schedules, ensuring alignment with the organization's strategic goals. ▪ Launching awareness campaigns to highlight the importance of key topics like resilience, digital trust, and cybersecurity. Involvement of senior leadership in training initiatives to demonstrate their commitment and support and use real-world scenarios to make the content practical and relatable. ▪ Implementation of mechanisms to measure the effectiveness of training programs through assessments, feedback surveys, and performance metrics. Regularly reviewing and updating training programs based on feedback and industry trends to ensure they remain relevant and effective.		
Article mapping			
AI ACT Ref#	▪ Article 4 ▪ Article 14.5	**GDPR Ref#**	▪ Article 39.1 ▪ Article 47.2
NIS2 Ref#	▪ Article 20.2 ▪ Article 21.2	**DORA Ref#**	▪ Article 5.2 ▪ Article 5.4 ▪ Article 13.6 ▪ Article 16.1

4.2. Compliance

Theme definition: Compliance involves the development and implementation of controls and mechanisms to adhere to regulatory requirements, manage risks effectively, and ensure organizational activities align with regulations and industry standards.

Sub-themes:

- Conformity assessment & periodically monitoring
- Authority cooperation

4.2.1. Sub-theme: Conformity assessment & periodically monitoring

Sub-theme definition: Conformity refers to the alignment and adherence to established legal and regulatory requirements, ensuring consistent operations across GDPR, AI Act, NIS2, and DORA.

<table>
<tr><th colspan="4">Design principle: 2.1 Conformity assessment & periodically monitoring</th></tr>
<tr><td>Theme</td><td>Compliance</td><td>Sub-theme</td><td>Conformity assessment & periodically monitoring</td></tr>
<tr><td>Design principle</td><td colspan="3">Organizations shall establish comprehensive conformity mechanisms including regular audits, continuous monitoring, and thorough documentation of compliance activities. These mechanisms shall integrate risk assessments, incident response plans, and stakeholder training to maintain ongoing regulatory compliance and operational resilience.</td></tr>
<tr><td>Implementation guidance</td><td colspan="3">▪ Establish Control Monitoring Mechanisms: Implement continuous monitoring tools and systems to track the effectiveness of controls. Set up automated alerts and reporting mechanisms to identify and address control deficiencies promptly.
▪ Conduct Control Testing and Validation: Perform regular testing and validation of controls to ensure they are functioning as intended. Use internal audits, external audits, and self-assessments to evaluate control effectiveness.
▪ Maintain Control Documentation: Document all controls, including their design, implementation, and monitoring processes. Keep records of control testing, validation results, and any corrective actions taken.
▪ Implement Control Review and Update Processes: Establish a schedule for regular review and updating of controls to address changes in regulatory requirements and business operations. Ensure controls remain relevant and effective in mitigating risks and ensuring compliance.
▪ Define internal audit plans and ensure appropriate follow up.</td></tr>
<tr><th colspan="4">Article mapping</th></tr>
<tr><td>AI ACT Ref#</td><td>▪ Article 17
▪ Article 18
▪ Article 19
▪ Article 42
▪ Article 43
▪ Article 44</td><td>GDPR Ref#</td><td>▪ Article 5.2
▪ Article 24.1
▪ Article 32.1
▪ Article 39.1</td></tr>
</table>

Design principle: 2.1 Conformity assessment & periodically monitoring			
	▪ Article 46 ▪ Article 47 ▪ Article 48 ▪ Article 72		
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ Article 5.2 ▪ Article 6.6 ▪ Article 6.7 ▪ Article 11.4 ▪ Article 11.6

4.2.2. Sub-theme: Authority cooperation

Sub-theme definition: Authority cooperation involves collaborative efforts and communications with regulatory bodies to ensure compliance and facilitate information exchange.

Design principle: 2.2 Authority cooperation			
Theme	Compliance	**Sub-theme**	Authority cooperation
Design principle	Organizations shall establish and maintain transparent and collaborative relationships with regulatory authorities to ensure compliance with applicable laws, regulations, and industry standards.		
Implementation guidance	▪ Organizations shall establish clear and structured communication channels with regulatory bodies to ensure timely and accurate information exchange. Processes should be in place to facilitate communication both upon request and in response to events. ▪ Organizations must maintain up-to-date documentation and records as required by regulatory authorities, ensuring that these are readily accessible and can be provided promptly upon request. ▪ Organizations shall actively engage with regulatory authorities during audits, investigations, and risk assessments. They must provide necessary access and information transparently and cooperatively. ▪ Following major incidents, organizations are required to collaborate with regulatory bodies to analyze causes, implement corrective actions, and enhance resilience. ▪ Authorized representatives must be empowered and equipped to act effectively on the organization's behalf in all regulatory interactions. ▪ Organizations shall ensure that timely and accurate communication between their third parties and competent authorities is contractually agreed upon, establishing clear expectations for cooperation.		
Article mapping			

Design principle: 2.2 Authority cooperation			
AI ACT Ref#	▪ Article 20 ▪ Article 21 ▪ Article 26.5	**GDPR Ref#**	▪ Article 27.4 ▪ Article 30.4 ▪ Article 31 ▪ Article 33.1 ▪ Article 36.1 ▪ Article 36.3 ▪ Article 37.7 ▪ Article 39.1
NIS2 Ref#	▪ Article 23.1 ▪ Article 23.4	**DORA Ref#**	▪ Article 19.1 ▪ Article 19.2 ▪ Article 35.5 ▪ Article 37.4

4.3. Risk management

Theme definition: Risk management is the systematic process of identifying, assessing, prioritizing, and mitigating risks to minimize their impact on an organization's objectives. It involves implementing strategies and controls to manage potential threats and uncertainties, ensuring organizational resilience and compliance with regulatory requirements.

Sub-themes:

- Risk governance
- Risk identification
- Risk assessment
- Risk response
- Risk reporting and monitoring
- Control frameworks

4.3.1. Sub-theme: Risk governance

Sub-theme definition: Risk governance is the framework of policies, procedures, and structures that ensure effective oversight and accountability in managing risks within an organization. It involves defining roles and responsibilities, establishing risk management processes, and integrating risk management into the organization's overall governance structure to support informed decision-making and regulatory compliance.

Design principle: 3.1 Risk governance			
Theme	Risk management	**Sub-theme**	Risk governance
Design principle	Organization shall establish a structured framework of policies, procedures, and organizational structures to ensure effective oversight and accountability in managing digital trust risks.		

Design principle: 3.1 Risk governance			
Implementation guidance	▪ A comprehensive risk governance policy should be created, detailing the principles, roles, responsibilities, and processes for managing digital trust risks within the organization. The policy should cover the broad scope of digital trust (e.g., systems/assets, network, people, data, third parties and premises). Organizations should ensure alignment with the organization's strategic goals, regulatory requirements and ensure the integration with its enterprise risk management framework. This policy should be approved by the management body and communicated to all relevant stakeholders. ▪ Establishment of risk governance structures by the means of risk committees or working groups that include representatives from key departments such as legal, compliance, finance, operations, and risk management. These committees should regularly review risk management activities and provide strategic direction. Additionally, roles and responsibilities for risk governance should be clearly defined and assigned. ▪ Integration of risk management into the organization's overall corporate governance structure, ensuring alignment with other governance activities such as strategic planning, financial reporting, and compliance. ▪ Determination of risk appetite and tolerance that defines the level of risk the organization is willing to accept in pursuit of its objectives. Additionally, risk tolerance levels for different types of risks should be established, providing guidelines for decision-making within the defined risk appetite. The management body should regularly review and approve the organization's risk management policies, risk appetite, and risk tolerance levels. ▪ Fostering a risk-aware culture by conducting tegular training and awareness programs to educate employees about risk management principles, policies, and procedures. Employees should understand their roles in managing risks. Organizations should promote open communication about risks, encouraging employees to report potential risks and issues without fear of retribution. ▪ Detailed records of all risk management activities, including risk assessments, risk registers, risk reports, and documentation of risk mitigation actions, should be maintained. Documentation should be easily accessible and support transparency and accountability. An audit trail of risk management activities should be kept to facilitate audits and reviews, ensuring that records are retained in accordance with regulatory and organizational requirements. ▪ Organizations should regularly review and update the risk governance framework and processes to ensure they remain relevant and effective. Feedback from stakeholders and lessons learned from past experiences should be incorporated. Staying informed about industry best practices, emerging trends, and regulatory changes is crucial for continuously enhancing risk governance capabilities. This information should be used to refine and improve the risk governance framework.		
Article mapping			
AI ACT Ref#	▪ Article 6 ▪ Article 8	**GDPR Ref#**	▪ Article 5.2 ▪ Article 24.1

Design principle: 3.1 Risk governance			
	▪ Article 9 ▪ Article 17		▪ Article 25 ▪ Article 26.1 ▪ Article 35.1 ▪ Article 35.7 ▪ Article 37 ▪ Article 38 ▪ Article 39.1
NIS2 Ref#	▪ Article 20 ▪ Article 21	**DORA Ref#**	▪ Article 5.1 ▪ Article 5.2 ▪ Article 5.3 ▪ Article 6.1 ▪ Article 6.2 ▪ Article 6.3 ▪ Article 6.4 ▪ Article 6.5 ▪ Article 6.6 ▪ Article 6.7 ▪ Article 6.8 ▪ Article 6.9 ▪ Article 6.10 ▪ Article 7.a ▪ Article 7.b ▪ Article 7.c ▪ Article 7.d ▪ Article 8.1 ▪ Article 8.2 ▪ Article 8.3 ▪ Article 8.4 ▪ Article 8.5 ▪ Article 8.6 ▪ Article 9.1 ▪ Article 9.2 ▪ Article 9.3 ▪ Article 9.4 ▪ Article 10.1 ▪ Article 10.2 ▪ Article 10.3

Design principle: 3.1 Risk governance			
			▪ Article 10.4 ▪ Article 12.1 ▪ Article 12.2 ▪ Article 12.3 ▪ Article 12.4 ▪ Article 12.6 ▪ Article 12.7 ▪ Article 24.1 ▪ Article 24.2 ▪ Article 24.3 ▪ Article 24.4 ▪ Article 24.5 ▪ Article 24.6 ▪ Article 28.1 ▪ Article 28.2

4.3.2. Sub-theme: Risk identification

Sub-theme definition: Risk identification is the process of systematically identifying potential events or conditions that could negatively impact an organization's objectives. It involves recognizing and documenting risks across various areas, such as operational, financial, strategic, and compliance, to enable proactive risk management and mitigation.

Design principle: 3.2 Risk identification			
Theme	Risk management	**Sub-theme**	Risk identification
Design principle	Organizations shall establish a systematic and comprehensive process for identifying potential digital trust risks across all areas of the organization.		
Implementation guidance	▪ Organizations shall establish standardized processes for identifying risks. This includes defining the steps and methodologies to be used, such as risk assessments, SWOT analysis, brainstorming sessions, and scenario planning. The processes should be documented and communicated to all relevant stakeholders to ensure consistency and understanding. ▪ Engagement of key stakeholders from different departments and levels of the organization in the risk identification process are needed to ensure a wide range of perspectives and expertise are considered in identifying potential risks. ▪ Organizations should use a variety of tools and techniques to identify risks. This includes conducting risk assessments, SWOT analysis (Strengths, Weaknesses, Opportunities, Threats), brainstorming sessions,		

Design principle: 3.2 Risk identification			
	interviews, surveys, and workshops. These tools and techniques help to systematically identify and document potential risks. ▪ A risk register should be developed to document identified risks. The risk register should include details such as the risk description, potential impact, likelihood, risk owner, and any existing controls or mitigation measures. The risk register should be regularly updated and reviewed to ensure it remains current and relevant. ▪ Identified risks should be categorized based on their nature, such as operational, financial, strategic, or compliance risks. Risks should also be prioritized based on their potential impact and likelihood. ▪ Organizations should conduct regular risk reviews to identify new risks and reassess existing risks. This includes periodic risk assessments, audits, and reviews of the risk register. Regular risk reviews ensure that the risk identification process remains dynamic and responsive to changes in the internal and external environment.		
Article mapping			
AI ACT Ref#	▪ Article 9.1 ▪ Article 9.2	**GDPR Ref#**	▪ Article 24.1 ▪ Article 25.1 ▪ Article 35.1 ▪ Article 35.7
NIS2 Ref#	▪ Article 20 ▪ Article 21	**DORA Ref#**	▪ Article 6.1 ▪ Article 6.2 ▪ Article 6.3 ▪ Article 6.4 ▪ Article 6.5 ▪ Article 6.6 ▪ Article 6.7 ▪ Article 6.8 ▪ Article 8.1 ▪ Article 8.2 ▪ Article 8.3 ▪ Article 8.4 ▪ Article 8.5 ▪ Article 8.6

4.3.3. Sub-theme: Risk assessment

Sub-theme definition: Risk assessment is the process of evaluating identified risks to determine their potential impact and likelihood, providing a basis for prioritizing and managing them. It involves analyzing the severity and probability of risks to inform decision-making and develop appropriate mitigation strategies.

Design principle: 3.3 Risk assessment			
Theme	Risk management	**Sub-theme**	Risk assessment
Design principle	Organizations shall establish a systematic and comprehensive process for evaluating identified digital trust risks to determine their potential impact and likelihood.		
Implementation guidance	▪ Organizations shall establish standardized processes for conducting risk assessments. This includes defining the steps and methodologies to be used, such as qualitative and quantitative analysis, risk matrices, scenario analysis. ▪ Organizations should use a variety of tools and techniques to assess risks. This includes conducting qualitative assessments to evaluate the severity and likelihood of risks, as well as quantitative assessments to measure the potential financial impact. Tools such as risk matrices, heat maps, and risk scoring models can help to systematically evaluate and prioritize risks. ▪ Risk assessments should be conducted regularly to evaluate identified risks related to digital trust. This includes analyzing the potential impact and likelihood of each risk, considering factors such as financial, operational, reputational, and regulatory implications. The results of the risk assessments should be documented in a risk register, including details such as risk descriptions, impact and likelihood ratings, and any existing controls or mitigation measures. ▪ Identified risks should be prioritized based on their assessed impact and likelihood. This helps to focus attention and resources on the most significant risks that could affect the organization. Prioritization can be done using risk matrices or risk scoring models to rank risks according to their severity and probability.		
Article mapping			
AI ACT Ref#	▪ Article 9.1 ▪ Article 9.2 ▪ Article 9.5 ▪ Article 9.6 ▪ Article 9.9 ▪ Article 9.10 ▪ Article 51.1 ▪ Article 51.2	**GDPR Ref#**	▪ Article 35.1 ▪ Article 35.2 ▪ Article 35.3 ▪ Article 35.4 ▪ Article 35.5 ▪ Article 35.6 ▪ Article 35.7 ▪ Article 35.8

Design principle: 3.3 Risk assessment			
	▪ Article 51.3 ▪ Article 55.1 ▪ Article 55.2 ▪ Article 55.3		▪ Article 35.9 ▪ Article 35.10 ▪ Article 35.11
NIS2 Ref#	▪ Article 20 ▪ Article 21	**DORA Ref#**	▪ Article 6.1 ▪ Article 6.2 ▪ Article 6.3 ▪ Article 6.4 ▪ Article 6.5 ▪ Article 6.6 ▪ Article 6.7 ▪ Article 6.8 ▪ Article 8.1 ▪ Article 8.2 ▪ Article 8.4 ▪ Article 8.5 ▪ Article 11.1 ▪ Article 11.2 ▪ Article 11.3 ▪ Article 24.1 ▪ Article 24.2 ▪ Article 24.3 ▪ Article 24.4 ▪ Article 24.5 ▪ Article 24.6

4.3.4. Sub-theme: Risk response

Sub-theme definition: Risk Response is the process of developing and implementing strategies to manage identified risks by reducing, transferring, avoiding, or accepting them. It involves selecting and applying appropriate measures to mitigate the impact and likelihood of risks, ensuring alignment with the organization's risk appetite and objectives.

Design principle: 3.4 Risk response			
Theme	Risk management	**Sub-theme**	Risk response
Design principle	Organizations shall establish a systematic and strategic approach for developing and implementing risk treatment measures to manage identified risks.		

Design principle: 3.4 Risk response	
Implementation guidance	▪ For each identified risk, organizations should identify potential treatment options. These options typically include risk avoidance, risk reduction, risk transfer, and risk acceptance. Each option should be evaluated based on its feasibility, effectiveness, and alignment with the organization's risk appetite and objectives. ▪ Organizations should evaluate the identified risk treatment options to determine the most appropriate measures for managing each risk. This evaluation should consider factors such as the potential impact and likelihood of the risk, the cost and benefits of the treatment measures, and the organization's risk tolerance. The selected risk treatment measures should be documented and approved by relevant stakeholders. ▪ For each selected risk treatment measure, organizations should develop detailed risk treatment plans. These plans should outline the specific actions to be taken, the resources required, the timeline for implementation, and the roles and responsibilities of individuals involved. The plans should also include performance indicators to measure the effectiveness of the treatment measures. ▪ Organizations should implement the selected risk treatment measures according to the developed plans. This includes allocating the necessary resources, assigning responsibilities, and ensuring that the actions are carried out as planned. Regular progress updates should be provided to relevant stakeholders to ensure transparency and accountability. ▪ Organizations should continuously monitor the effectiveness of the implemented risk treatment measures. This includes tracking performance indicators, conducting regular reviews, and assessing whether the measures are achieving the desired outcomes. Any deviations or issues should be addressed promptly, and adjustments should be made as needed to ensure the effectiveness of the treatment measures. ▪ Detailed records of all risk treatment activities should be maintained, including the identified treatment options, selected measures, treatment plans, and implementation progress. Documentation should be easily accessible and support transparency and accountability. An audit trail of risk treatment activities should be kept to facilitate audits and reviews. ▪ Organizations should ensure that relevant stakeholders are informed about risk treatment activities. This includes providing regular updates on the progress and effectiveness of the treatment measures, as well as any changes or adjustments made. Clear communication channels should be established to facilitate the sharing of information and feedback. ▪ Organizations should regularly review and update the risk treatment framework and processes to ensure they remain relevant and effective. Feedback from stakeholders and lessons learned from past experiences should be incorporated. Staying informed about industry best practices, emerging trends, and regulatory changes is crucial for continuously enhancing risk treatment capabilities.

Article mapping			
AI ACT Ref#	▪ Article 9.2 ▪ Article 9.3 ▪ Article 9.6	**GDPR Ref#**	▪ Article 35.1 ▪ Article 35.2 ▪ Article 35.3

Design principle: 3.4 Risk response			
	▪ Article 9.9		▪ Article 35.4 ▪ Article 35.5 ▪ Article 35.6 ▪ Article 35.7 ▪ Article 35.8 ▪ Article 35.9 ▪ Article 35.10 ▪ Article 35.11
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ Article 5.2 ▪ Article 6.1 ▪ Article 6.2 ▪ Article 6.3 ▪ Article 6.8 ▪ Article 8.1 ▪ Article 8.2 ▪ Article 8.4 ▪ Article 8.5 ▪ Article 9.1 ▪ Article 9.2 ▪ Article 9.3 ▪ Article 9.4 ▪ Article 13.3 ▪ Article 24.1 ▪ Article 24.2 ▪ Article 24.3 ▪ Article 24.4 ▪ Article 24.5 ▪ Article 24.6

4.3.5. Sub-theme: Risk reporting & monitoring

Sub-theme definition: Risk reporting and monitoring involve the continuous process of tracking identified risks and their mitigation measures, and regularly communicating the status and effectiveness of risk management activities to relevant stakeholders. This process ensures transparency, supports informed decision-making, and enables timely adjustments to risk management strategies.

Design principle: 3.5 Risk Reporting & Monitoring			
Theme	Risk management	**Sub-theme**	Risk reporting & monitoring

Design principle: 3.5 Risk Reporting & Monitoring	
Design principle	Organizations shall establish a systematic and continuous process for tracking identified risks, monitoring the effectiveness of mitigation measures, and regularly communicating risk status to relevant stakeholders.
Implementation guidance	▪ Organizations should establish standardized processes for risk reporting and monitoring. This includes defining the steps and methodologies to be used, such as key risk indicators (KRIs), risk dashboards, and regular risk reviews. The processes should be documented and communicated to all relevant stakeholders to ensure consistency and understanding. ▪ Organizations should identify and define key risk indicators (KRIs) that are critical to monitoring the status and effectiveness of risk management activities. KRIs should be aligned with the organization's risk appetite and strategic objectives. These indicators should be regularly tracked and reported to provide early warning signs of potential risk issues. ▪ Organizations should implement mechanisms for continuously monitoring identified risks and their mitigation measures. Regular risk assessments and audits should also be conducted to ensure ongoing oversight. ▪ Standardized reporting templates and tools should be developed to ensure consistency and comprehensiveness in risk reporting. These templates should include fields for key metrics, risk status, mitigation measures, and any issues or deviations. ▪ Organizations should establish specific timelines and frequency for risk reporting. This includes defining the intervals at which risk reports should be generated (e.g., monthly, quarterly) and the deadlines for submission. Regular reporting ensures that risk information is up-to-date and relevant for decision-making. ▪ Clear responsibilities for preparing, reviewing, and submitting risk reports should be assigned within the organization. This includes designating individuals or teams responsible for collecting risk data, analyzing it, and preparing reports. ▪ Organizations should ensure that relevant stakeholders are informed about risk status and management activities. This includes providing regular updates to senior management, the management body, and other key stakeholders. Clear communication channels should be established to facilitate the sharing of risk information and feedback. ▪ Organizations should continuously monitor the effectiveness of implemented risk mitigation measures. This includes tracking performance indicators, conducting regular reviews, and assessing whether the measures are achieving the desired outcomes. Any deviations or issues should be addressed promptly, and adjustments should be made as needed. ▪ Detailed records of all risk reporting and monitoring activities should be maintained, including risk reports, monitoring logs, and documentation of KRIs and mitigation measures. Documentation should be easily accessible and support transparency and accountability. An audit trail of risk reporting and monitoring activities should be kept to facilitate audits and reviews.

Design principle: 3.5 Risk Reporting & Monitoring			
	▪ Organizations should regularly review and update the risk reporting and monitoring framework and processes to ensure they remain relevant and effective. Feedback from stakeholders and lessons learned from past experiences should be incorporated. Staying informed about industry best practices, emerging trends, and regulatory changes is crucial for continuously enhancing risk reporting and monitoring capabilities.		
Article mapping			
AI ACT Ref#	▪ Article 17.1 ▪ Article 72 ▪ Article 73 ▪ Article 82	**GDPR Ref#**	▪ Article 24.1
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ Article 5.1 ▪ Article 5.2 ▪ Article 5.3 ▪ Article 6.1 ▪ Article 6.4 ▪ Article 6.5 ▪ Article 6.6 ▪ Article 6.7 ▪ Article 6.8 ▪ Article 8.1 ▪ Article 8.2 ▪ Article 9.1 ▪ Article 13.4 ▪ Article 13.7 ▪ Article 17.2 ▪ Article 24.1 ▪ Article 24.6 ▪ Article 28.2 ▪ Article 29.2

4.3.6. Sub-theme: Control frameworks

Sub-theme definition: A structured set of guidelines and processes designed to ensure effective governance, risk management, and compliance to applicable laws and regulations within an organization.

<table>
<tr><th colspan="4">Design principle: 3.6 Control frameworks</th></tr>
<tr><td>Theme</td><td>Risk management</td><td>Sub-theme</td><td>Control frameworks</td></tr>
<tr><td>Design principle</td><td colspan="3">Organizations shall create and maintain a robust control framework that includes clearly defined control objectives. Regular testing, validation, and updating of controls, along with assigning ownership and providing training, are essential to mitigate risks and maintain regulatory compliance.</td></tr>
<tr><td>Implementation guidance</td><td colspan="3">▪ Define control objectives: Identify specific control objectives aligned with the requirements of NIS2, DORA, AI Act, and GDPR. Ensure control objectives cover areas such as data protection, cybersecurity, operational resilience, and AI governance.
▪ Develop control policies and procedures: Create detailed policies and procedures that outline the controls needed to meet regulatory requirements. Ensure these documents are accessible, regularly updated, and communicated to relevant stakeholders.
▪ Design and implement controls: Develop and implement technical, administrative, and physical controls to address identified control objectives. Ensure controls are designed to mitigate risks and ensure compliance with regulatory standards.
▪ Assign control ownership: Designate control owners responsible for the implementation, monitoring, and maintenance of each control. Ensure control owners have the necessary resources and authority to effectively manage their controls.</td></tr>
<tr><th colspan="4">Article mapping</th></tr>
<tr><td>AI ACT Ref#</td><td>The AI Act does not refer to a control framework. Nevertheless, requirements from the Act, particularly with regards to high-risk AI systems, might be included as controls by organizations evaluating compliance with the regulation:
▪ Article 9.1
▪ Article 9.2
▪ Article 9.5
▪ Article 9.6
▪ Article 9.8
▪ Article 17.1</td><td>GDPR Ref#</td><td>▪ Article 5.2
▪ Article 24.1
▪ Article 24.2
▪ Article 25.1
▪ Article 31.2
▪ Article 35.7
▪ Article 39.1</td></tr>
</table>

Design principle: 3.6 Control frameworks			
NIS2 Ref#	▪ Article 20.1 ▪ Article 20.2 ▪ Article 21.1 ▪ Article 21.2 ▪ Article 21.4	**DORA Ref#**	▪ Article 5.1 ▪ Article 5.2 ▪ Article 5.3 ▪ Article 5.4 ▪ Article 6.1 ▪ Article 6.2 ▪ Article 6.3 ▪ Article 6.4 ▪ Article 6.5 ▪ Article 6.6 ▪ Article 6.7 ▪ Article 6.8 ▪ Article 9.4

4.4. Architecture

Theme definition: Business and IT architecture is the comprehensive framework for designing, implementing, and managing an organization's business processes and IT infrastructure. This architecture ensures the alignment of technological systems and business operations with organizational objectives, emphasizing security, data protection, and operational resilience. This unified approach includes defining business processes and functions, assigning ownership, and validating outcomes to achieve a robust and compliant operational environment.

Sub-themes:

- Formalizing the business architecture (functions, processes)
- Identifying IT assets & systems

4.4.1. Sub-theme: Formalizing the business architecture (functions, processes)

Sub-theme definition: Understanding processes/functions involves a comprehensive knowledge and documentation of organizational operations and their impact on compliance and security under regulations.

Design principle: 4.1 Formalizing the business architecture (functions, processes)			
Theme	Architecture	**Sub-theme**	Formalizing the business architecture (functions, processes)
Design principle	Organizations shall identify and classify all business functions and processes based on their criticality. Assign business ownership to each function and process and require business owners to validate the classification outcomes to ensure accuracy and accountability.		

Design principle: 4.1 Formalizing the business architecture (functions, processes)			
Implementation guidance	▪ Identify critical functions and processes: Conduct a comprehensive assessment to identify all functions and processes within the organization. Engage stakeholders from various departments to ensure all critical functions are captured. ▪ Identify business owners for each function and process to ensure accountability and ownership. ▪ Categorize based on criticality: Use business impact analysis (BIA) to determine the importance of each function and process. Classify functions and processes into categories such as critical, important, and non-critical. Define criteria for categorization based on factors like impact on operations, regulatory requirements, and customer service. ▪ Ensure business owners validate the categorization outcomes to confirm accuracy and relevance.		
Article mapping			
AI ACT Ref#	▪ N/A	**GDPR Ref#**	▪ Article 30.1 ▪ Article 30.2 ▪ Article 30.3 ▪ Article 30.5
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ Article 8.1 ▪ Article 8.5 ▪ Article 8.6

4.4.2. Sub-theme: Identifying IT assets & systems

Sub-theme definition: Knowing your key assets involves identifying and managing critical organizational resources to protect them from risks and ensure their integrity.

Design principle: 4.2 Identifying IT assets & systems			
Theme	Architecture	**Sub-theme**	Identifying IT assets & systems
Design principle	Organizations shall conduct a comprehensive inventory of IT assets and map them to business functions and processes to get an accurate overview of their technology stack. They shall assign ownership, validate the mapping with stakeholders, and regularly review and update the documentation to maintain accuracy and support operational resilience.		
Implementation guidance	▪ Conduct an inventory of IT assets: Compile a comprehensive list of all IT assets, including hardware, software, networks, and AI systems. Ensure the inventory includes details such as asset type, location, ownership, and current usage. ▪ Map IT assets to business functions and processes: Establish a clear relationship between each IT asset and the business functions and processes they support. Create a mapping matrix or diagram to visualize the connections between IT assets and business operations.		

Design principle: 4.2 Identifying IT assets & systems			
	▪ Regularly review and update: Establish a process for regular review and updates of the IT asset mapping to reflect changes in the organization. Schedule periodic audits to ensure the mapping remains accurate and up to date. ▪ Leverage technology for automation: Utilize asset management and mapping tools to automate the identification and mapping process. Implement AI-driven solutions to enhance the accuracy and efficiency of the mapping.		
Article mapping			
AI ACT Ref#	The AI Act does not include any direct specifications on the existence of an AI inventory. However, it indirectly expects organizations to know about the existence of all AI systems in place, as well as their AI Act-specific risk classification and AI Act-specific role for each system: ▪ Article 9 ▪ Article 11	**GDPR Ref#**	▪ Article 30.1 ▪ Article 30.2 ▪ Article 30.3 ▪ Article 30.5
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ Article 8.1 ▪ Article 8.4 ▪ Article 8.6

4.5. Security

Theme definition: Security is the practice of protecting an organization's assets, including information, systems, and physical infrastructure, from threats and unauthorized access. It involves implementing measures such as policies, procedures, technologies, and controls to ensure confidentiality, integrity, authenticity and availability of critical resources.

Sub-themes:

- Organizational controls
- Technical security
- People controls
- Physical controls

4.5.1. Sub-theme: Organizational controls

Sub-theme definition: Organizational controls in the context of security are the policies, procedures, and practices implemented to safeguard an organization's assets and ensure compliance with security standards. These controls help manage and mitigate risks by establishing clear guidelines for protecting information, systems, and physical infrastructure from threats and unauthorized access. Organizational control involves the policies, procedures, and practices that ensure security measures are effectively

implemented and maintained within an organization. It includes the assignment of roles and responsibilities, the establishment of security policies, and the continuous monitoring and improvement of security practices.

Design principle: 5.1 Organizational controls			
Theme	Security	**Sub-theme**	Organizational controls
Design principle	Organizations shall establish comprehensive and robust organizational controls, including policies, procedures, and practices, to safeguard the organization's assets and ensure compliance with security standards.		
Implementation guidance	▪ Organizations should create a comprehensive security policy framework that outlines the principles, objectives, and scope of security controls. This framework should align with the organization's strategic goals, risk management practices, and regulatory requirements. The framework should include guidelines for protecting information, systems, and physical infrastructure from threats and unauthorized access. ▪ Organizations should develop and implement detailed security policies and procedures that cover various aspects of security, including access control, data protection, incident response, and physical security. These policies and procedures should be documented and communicated to all relevant stakeholders to ensure consistency and understanding. ▪ Clear roles and responsibilities for implementing and maintaining security controls should be defined and assigned within the organization. This includes designating a Chief Information Security Officer (CISO) or equivalent role to oversee the security function and ensure accountability across the organization. Security responsibilities should be integrated into job descriptions and performance evaluations. ▪ Organizations should conduct regular risk assessments to identify potential security threats and vulnerabilities. This includes evaluating the likelihood and impact of security risks and documenting the findings in a risk register. Risk assessments should be used to inform the development and implementation of security controls. ▪ Regular security training and awareness programs should be conducted to educate employees about security policies, procedures, and best practices. Employees should be trained on how to recognize and respond to security threats, and their roles in maintaining the organization's security posture. Training should be tailored to different roles and responsibilities within the organization. ▪ Organizations should continuously monitor the effectiveness of implemented security controls. This includes using security monitoring tools, conducting regular audits, and reviewing security logs and reports. Any deviations or issues should be addressed promptly, and adjustments should be made as needed to ensure the effectiveness of the controls. ▪ Detailed records of all security activities should be maintained, including security policies, risk assessments, incident reports, and documentation of security controls. Documentation should be easily accessible and support transparency and accountability. An audit trail of security activities should be kept to facilitate audits and reviews.		

<table>
<tr><th colspan="4">Design principle: 5.1 Organizational controls</th></tr>
<tr><td></td><td colspan="3">▪ Organizations should ensure that relevant stakeholders are informed about security activities and the status of security controls. This includes providing regular updates to senior management, the management body and other key stakeholders. Clear communication channels should be established to facilitate the sharing of security information and feedback.
▪ Organizations should regularly review and update the security policy framework and controls to ensure they remain relevant and effective. Feedback from stakeholders and lessons learned from past experiences should be incorporated. Staying informed about industry best practices, emerging threats, and regulatory changes is crucial for continuously enhancing security capabilities.</td></tr>
<tr><th colspan="4">Article mapping</th></tr>
<tr><td>AI ACT Ref#</td><td>The AI Act does not refer to the implementation of organizational controls. Nevertheless, the following articles can be linked to requirements that could be associated with organizational controls:
▪ Article 9
▪ Article 17
▪ Article 72</td><td>GDPR Ref#</td><td>▪ Article 5.1
▪ Article 24.1
▪ Article 25.1
▪ Article 28.1
▪ Article 28.3
▪ Article 32.1
▪ Article 32.2
▪ Article 32.4
▪ Article 35.1
▪ Article 35.7</td></tr>
<tr><td>NIS2 Ref#</td><td>▪ Article 21.1
▪ Article 21.2
▪ Article 21.3
▪ Article 21.4</td><td>DORA Ref#</td><td>▪ Article 5.1
▪ Article 5.2
▪ Article 5.4
▪ Article 6.1
▪ Article 6.2
▪ Article 6.3
▪ Article 6.4
▪ Article 8
▪ Article 9
▪ Article 10.1
▪ Article 10.2
▪ Article 10.3
▪ Article 11.1
▪ Article 11.2
▪ Article 11.3
▪ Article 11.4
▪ Article 11.5</td></tr>
</table>

Design principle: 5.1 Organizational controls			
			▪ Article 11.6 ▪ Article 11.7 ▪ Article 11.8 ▪ Article 12.1 ▪ Article 12.2 ▪ Article 12.4 ▪ Article 13.1 ▪ Article 13.2 ▪ Article 13.3 ▪ Article 13.6 ▪ Article 14.1 ▪ Article 14.2 ▪ Article 14.3

4.5.2. Sub-theme: Technical security

Sub-theme definition: Technical security refers to the implementation of technology-based measures and controls designed to protect an organization's information systems, networks, and data from unauthorized access, breaches, and other cyber threats. These measures include firewalls, encryption, intrusion detection systems, access controls, and other technologies that ensure the confidentiality, integrity, authenticity and availability of critical resources.

Design principle: 5.2 Technical security			
Theme	Security	**Sub-theme**	Technical security
Design principle	Organizations shall implement robust and comprehensive technology-based measures and controls to protect the organization's information systems, networks, and data from unauthorized access, breaches, and other cyber threats.		
Implementation guidance	▪ Organizations should create a comprehensive technical security framework that outlines the principles, objectives, and scope of technical security measures. This framework should align with the organization's strategic goals, risk management practices, and regulatory requirements. The framework should include guidelines for protecting information systems, networks, and data from cyber threats. ▪ Organizations should conduct a thorough security assessment to identify potential vulnerabilities and threats to their information systems, networks, and data. This assessment should include penetration testing, vulnerability scanning, and risk assessments. The findings should be documented and used to inform the development and implementation of technical security measures. ▪ Organizations should implement robust access controls to ensure that only authorized individuals have access to sensitive information and		

Design principle: 5.2 Technical security	
	systems. This includes using multi-factor authentication (MFA), role-based access control (RBAC), and least privilege principles. Access controls should be regularly reviewed and updated to ensure their effectiveness. ▪ Firewalls and intrusion detection systems (IDS) should be deployed to monitor and control incoming and outgoing network traffic. These systems help to detect and prevent unauthorized access and potential cyber threats. Regular updates and maintenance should be performed to ensure their continued effectiveness. ▪ Organizations should use encryption to protect sensitive data both at rest and in transit. This includes encrypting data stored on servers, databases, and storage devices, as well as data transmitted over networks. Strong encryption algorithms and key management practices should be implemented to ensure data security. ▪ Endpoint security measures should be implemented to protect devices such as computers, mobile devices, and servers from cyber threats. This includes using antivirus software, endpoint detection and response (EDR) solutions, and regular patch management to keep systems up-to-date and secure. ▪ Organizations should establish network security measures to protect their internal and external networks. This includes segmenting networks, using virtual private networks (VPNs) for secure remote access, and implementing secure network protocols. Regular network monitoring and analysis should be conducted to detect and respond to potential threats. ▪ Organizations should continuously monitor the effectiveness of implemented technical security measures. This includes using security information and event management (SIEM) systems, conducting regular audits, and reviewing security logs and reports. Any deviations or issues should be addressed promptly, and adjustments should be made as needed to ensure the effectiveness of the measures.)

Article mapping			
AI ACT Ref#	The AI Act does not refer to the implementation of technical security measures or controls. Nevertheless, the following articles can be linked to requirements that could be associated with technical controls: ▪ Article 15 ▪ Article 17 ▪ Article 26	**GDPR Ref#**	▪ Article 5.1 ▪ Article 24.1 ▪ Article 25.1 ▪ Article 28.1 ▪ Article 28.3 ▪ Article 32.1 ▪ Article 32.2 ▪ Article 32.4 ▪ Article 35.1 ▪ Article 35.7
NIS2 Ref#	▪ Article 21.1 ▪ Article 21.2 ▪ Article 21.3	**DORA Ref#**	▪ Article 5.1 ▪ Article 5.2 ▪ Article 6.2

Design principle: 5.2 Technical security			
	▪ Article 21.4		▪ Article 6.3 ▪ Article 6.8 ▪ Article 7 ▪ Article 8.2 ▪ Article 8.7 ▪ Article 9 ▪ Article 10.1 ▪ Article 10.2 ▪ Article 10.3 ▪ Article 12.1 ▪ Article 12.2 ▪ Article 12.3 ▪ Article 12.4 ▪ Article 12.7 ▪ Article 13.1 ▪ Article 13.3 ▪ Article 13.4

4.5.3. Sub-theme: People controls

Sub-theme definition: People controls in the context of security refer to the policies, procedures, and practices designed to manage and mitigate risks associated with human behavior and actions within an organization. These controls include background checks, access controls, security training, and awareness programs to ensure that employees and other stakeholders adhere to security protocols and contribute to the organization's overall security posture.

Design principle: 5.3 People controls			
Theme	Security	**Sub-theme**	People controls
Design principle	Organizations shall implement comprehensive policies, procedures, and practices to manage and mitigate risks associated with human behavior and actions within the organization.		
Implementation guidance	▪ Organizations should create a comprehensive framework that outlines the principles, objectives, and scope of people controls. This framework should align with the organization's strategic goals, risk management practices, and regulatory requirements. The framework should include guidelines for managing and mitigating risks associated with human behavior and actions. At least, the framework should contain the following:		

Design principle: 5.3 People controls	
	▪ Organizations should implement background checks and screening processes for all employees, contractors, and third-party vendors. This includes verifying employment history, criminal records, and qualifications to ensure that individuals with access to sensitive information and systems are trustworthy and reliable. ▪ Clear roles and responsibilities for security-related activities should be defined and assigned within the organization. This includes designating security roles such as Information Security Officer, Security Manager, and Security Awareness Coordinator. Security responsibilities should be integrated into job descriptions and performance evaluations. ▪ Organizations should foster a culture of security awareness by promoting open communication about security risks and encouraging employees to report potential security issues. Security awareness campaigns, workshops, and regular communications should be used to reinforce the importance of security and the role of employees in protecting the organization. ▪ Organizations should continuously monitor the effectiveness of implemented people controls. This includes conducting regular audits, reviewing access logs, and assessing compliance with security policies and procedures. Any deviations or issues should be addressed promptly, and adjustments should be made as needed to ensure the effectiveness of the controls. ▪ Detailed records of all people control activities should be maintained, including background checks, training records, access logs, and incident reports. Documentation should be easily accessible and support transparency and accountability. An audit trail of people control activities should be kept to facilitate audits and reviews. ▪ Organizations should ensure that relevant stakeholders are informed about people control activities and the status of security measures. This includes providing regular updates to senior management, the management body, and other key stakeholders. Clear communication channels should be established to facilitate the sharing of security information and feedback. ▪ Regular security training and awareness programs should be conducted to educate employees about physical security measures, best practices, and their roles in maintaining the organization's security posture. Employees should be trained on how to recognize and respond to physical security threats, and their responsibilities in protecting physical assets and facilities.

Article mapping			
AI ACT Ref#	The AI Act does not refer to the implementation of people controls. Nevertheless, the following articles can be linked to requirements that could be associated with people controls: ▪ Article 4 ▪ Article 14 ▪ Article 17	**GDPR Ref#**	The GDPR does not refer to the implementation of people controls. Nevertheless, the following articles can be linked to requirements that could be associated with people controls: ▪ Article 24.1 ▪ Article 24.2 ▪ Article 25.2 ▪ Article 32.1

Design principle: 5.3 People controls			
			▪ Article 32.4
NIS2 Ref#	▪ Article 20.1 ▪ Article 20.2 ▪ Article 21.2	**DORA Ref#**	▪ Article 5.2 ▪ Article 5.4 ▪ Article 13.6 ▪ Article 14.2

4.5.4. Sub-theme: Physical controls

Sub-theme definition: Physical controls in the context of security refer to the measures and mechanisms implemented to protect an organization's physical assets, facilities, and personnel from unauthorized access, damage, or theft. These controls include security guards, access control systems, surveillance cameras, and environmental safeguards to ensure the safety and security of the organization's physical environment.

Design principle: 5.4 Physical controls			
Theme	Security	**Sub-theme**	Physical controls
Design principle	Organizations shall implement comprehensive and robust physical controls to protect the organization's physical assets, facilities, and personnel from unauthorized access, damage, or theft.		
Implementation guidance	▪ Organizations should start by creating a comprehensive physical security framework that outlines the principles, objectives, and scope of physical controls. This framework should align with the organization's strategic goals, risk management practices, and regulatory requirements. The framework should include guidelines for protecting physical assets, facilities, and personnel from unauthorized access, damage, or theft. ▪ Organizations should conduct a thorough physical security assessment to identify potential vulnerabilities and threats to their facilities and assets. This assessment should include evaluating access points, perimeter security, environmental controls, and existing physical security measures. The findings should be documented and used to inform the development and implementation of physical controls. ▪ Organizations should implement robust access control systems to ensure that only authorized individuals have access to sensitive areas and facilities. This includes using key card systems, biometric authentication, and secure entry points. Access control systems should be regularly reviewed and updated to ensure their effectiveness. ▪ Surveillance and monitoring systems, such as security cameras and motion detectors, should be deployed to monitor and record activities within and around the organization's facilities. These systems help to detect and deter unauthorized access and potential security threats. Regular maintenance and monitoring should be performed to ensure their continued effectiveness. ▪ Organizations should employ security personnel, such as security guards and patrols, to monitor and protect their facilities. Security personnel		

Design principle: 5.4 Physical controls			
	should be trained in security protocols, emergency response, and incident reporting. Their presence can act as a deterrent to potential threats and provide a rapid response to security incidents. ▪ Organizations should establish perimeter security measures to protect the outer boundaries of their facilities. This includes using fences, gates, barriers, and security lighting to prevent unauthorized access. Perimeter security should be regularly inspected and maintained to ensure its effectiveness. ▪ Environmental controls should be implemented to protect physical assets and facilities from environmental threats such as fire, flooding, and extreme weather. This includes using fire suppression systems, water leak detection, and climate control systems. Regular testing and maintenance should be conducted to ensure these controls are functioning properly. ▪ Organizations should develop and implement emergency response plans that outline the steps to be taken in the event of a physical security breach or incident. The plans should include procedures for evacuation, lockdown, and communication with emergency services. Regular drills and simulations should be conducted to test the effectiveness of the emergency response plans. ▪ Organizations should continuously monitor the effectiveness of implemented physical controls. This includes conducting regular audits, reviewing access logs, and assessing compliance with physical security policies and procedures. Any deviations or issues should be addressed promptly, and adjustments should be made as needed to ensure the effectiveness of the controls. ▪ Detailed records of all physical security activities should be maintained, including security assessments, incident reports, and documentation of physical controls. Documentation should be easily accessible and support transparency and accountability. An audit trail of physical security activities should be kept to facilitate audits and reviews. ▪ Organizations should ensure that relevant stakeholders are informed about physical security activities and the status of security measures. This includes providing regular updates to senior management, the management body, and other key stakeholders. Clear communication channels should be established to facilitate the sharing of security information and feedback.		
Article mapping			
AI ACT Ref#	▪ N/A The AI Act does not refer to a physical controls. Nevertheless, requirements from the Act, particularly with regards to high-risk AI systems, might have to include physical security/access requirements by	**GDPR Ref#**	▪ Article 5.1 ▪ Article 32.1 ▪ Article 32.2

Design principle: 5.4 Physical controls			
	organizations evaluating compliance with the regulation.		
NIS2 Ref#	▪ Article 21.1 ▪ Article 21.2	**DORA Ref#**	▪ Article 6.2 ▪ Article 9.4

4.6. Continuity & resilience

Theme definition: Continuity and resilience refer to an organization's ability to maintain essential functions and quickly recover from disruptions, ensuring minimal impact on operations and stakeholders. This involves proactive planning, risk management, and adaptive strategies to withstand and respond to adverse events effectively.

Sub-themes:

- Resilience governance & oversight
- Minimal viable organization
- Resilience strategy & planning
- Resilience capabilities
- Resilience monitoring & assessment

4.6.1. Sub-theme: Resilience governance & oversight

Sub-theme definition: Resilience governance and oversight refer to the structured framework and processes established to ensure an organization's ability to anticipate, prepare for, respond to, and recover from adverse events. It involves the implementation of policies, procedures, and controls to manage risks, maintain operational continuity, and safeguard the organization's assets and stakeholders.

Design principle: 6.1 Resilience governance & oversight			
Theme	Continuity & resilience	**Sub-theme**	Resilience governance & oversight
Design principle	Resilience governance and oversight shall be assigned to the Management Body of the organization and they shall ensure the establishment of a comprehensive resilience framework.		
Implementation guidance	▪ Ensuring a comprehensive resilience framework is in place that covers both business continuity as well as disaster recovery outlining the policies, procedures, and standards for managing risks and ensuring business continuity. This framework should align with the organization's overall strategic objectives and regulatory requirements. ▪ Clearly defining and assigning roles and responsibilities for resilience governance and oversight. This includes appointing a resilience officer or team responsible for coordinating resilience activities and ensuring accountability across the organization. ▪ Ensuring the performance of regular risk assessments to identify potential threats and vulnerabilities that could impact the organization's operations. These assessments are used to prioritize risks and develop mitigation strategies.		

Design principle: 6.1 Resilience governance & oversight			
	▪ Periodically reviews and updates the governance structures to ensure they remain effective and aligned with the evolving risk landscape. This includes revising policies, procedures, and oversight mechanisms as needed.		
Article mapping			
AI ACT Ref#	▪ N/A The AI Act does not refer to a resilience governance & oversight. Nevertheless, requirements from the Act, particularly with regards reporting of incidents for high-risk AI systems, might have to include resilience governance & oversight requirements by organizations evaluating compliance with the regulation.	**GDPR Ref#**	▪ N/A
NIS2 Ref#	▪ Article 20.1	**DORA Ref#**	▪ Article 5.1 ▪ Article 5.2 ▪ Article 6.1 ▪ Article 6.4 ▪ Article 6.8

4.6.2. Sub-theme: Minimal viable organization

Sub-theme definition: A minimal viable organization (MVO) in the context of operational resilience is a lean and agile entity designed to maintain essential functions and deliver core services despite disruptions. It emphasizes streamlined processes, critical resource allocation, and adaptive strategies to ensure continuity and rapid recovery from adverse events.

Design principle: 6.2 Minimal viable organization			
Theme	Continuity & resilience	**Sub-theme**	Minimal viable organization
Design principle	The organization shall be designed to operate with the essential resources, processes, and personnel required to deliver its core value proposition effectively, ensuring operational efficiency, agility, and resilience.		

Design principle: 6.2 Minimal viable organization			
Implementation guidance	▪ Determining the essential functions and services that are critical to the organization's mission and value proposition. Focus should be on what is absolutely necessary to maintain operations and deliver value to customers. ▪ Identification and allocation of the minimum necessary resources, including personnel, technology, third parties, premises, data and financial assets, to support the core functions. Prioritization of resources that enhance the organization's ability to respond to and recover from disruptions. ▪ Involving key stakeholders, including customers, suppliers, and partners, in the resilience planning process. Maintain clear communication and collaboration to ensure alignment and support for the MVO's core functions. ▪ Periodically reviewing the MVO's structure, processes, and resilience plan to ensure they remain effective and aligned with the organization's goals. Adapt and refine the MVO as needed to address emerging risks and opportunities.		
Article mapping			
AI ACT Ref#	▪ N/A	**GDPR Ref#**	▪ N/A
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ Article 8.4 ▪ Article 8.5 ▪ Article 7.c ▪ Article 9.2 ▪ Article 9.3 ▪ Article 11.2 ▪ Article 11.4 ▪ Article 11.6 ▪ Article 12.1 ▪ Article 12.2 ▪ Article 12.4 ▪ Article 12.5 ▪ Article 12.6

4.6.3. Sub-theme: Resilience strategy & planning

Sub-theme definition: Resilience strategy and planning involve developing and implementing comprehensive approaches to ensure an organization's ability to anticipate, withstand, respond to, and recover from disruptions. It encompasses identifying potential risks, establishing mitigation measures, and creating actionable plans to maintain operational continuity and safeguard critical assets.

Design principle: 6.3 Resilience strategy & planning			
Theme	Continuity & resilience	**Sub-theme**	Resilience strategy & planning
Design principle	The organization shall integrate resilience into the organizational design by developing and implementing comprehensive strategies and plans that ensure the ability to anticipate, withstand, respond to, and recover from disruptions.		
Implementation guidance	▪ Identification and evaluation of potential risks and vulnerabilities that could impact the organization. Considering a wide range of scenarios, including natural disasters, cyber threats, supply chain disruptions, and other operational risks. ▪ Establishment of clear and measurable objectives for resilience that align with the organization's overall strategic goals. These objectives should focus on maintaining critical functions, minimizing downtime, and ensuring rapid recovery. ▪ Implementation of measures to mitigate identified risks and vulnerabilities. This could include diversifying suppliers, enhancing cybersecurity, improving infrastructure, and establishing backup systems. ▪ Development of detailed and actionable plans for responding to and recovering from disruptions. These plans should include clear roles and responsibilities, communication protocols, and step-by-step procedures for different types of incidents. The plan should outline strategies for maintaining core functions during adverse events, include business continuity, disaster recovery, and crisis management components tailored to the MVO's streamlined structure. ▪ Involving key stakeholders, including employees, customers, suppliers, and regulators, in the resilience planning process. Ensure open communication and collaboration to build a shared understanding and commitment to resilience. ▪ Regularly testing and validating resilience plans through simulations, drills, and exercises. Use these tests to identify gaps and areas for improvement, and update plans accordingly.		
Article mapping			
AI ACT Ref#	▪ Article 15.1 ▪ Article 15.5	**GDPR Ref#**	▪ Article 5.1 ▪ Article 32.1 ▪ Article 32.2

Design principle: 6.3 Resilience strategy & planning			
NIS2 Ref#	▪ Article 21	**DORA Ref#**	▪ Article 5.2 ▪ Article 6.8 ▪ Article 9.2 ▪ Article 11.2 ▪ Article 11.3 ▪ Article 11.4 ▪ Article 11.5 ▪ Article 11.6 ▪ Article 11.7 ▪ Article 12.1 ▪ Article 12.4 ▪ Article 12.6 ▪ Article 14.1 ▪ Article 14.2

4.6.4. Sub-theme: Resilience capabilities

Sub-theme definition: Resilience capabilities refer to the specific skills, resources, and processes that enable an organization to effectively anticipate, withstand, respond to, and recover from disruptions. These capabilities encompass areas such as risk management, business continuity, crisis management, and adaptive capacity, ensuring the organization can maintain operational stability and quickly return to normalcy.

Design principle: 6.4 Resilience capabilities			
Theme	Continuity & resilience	**Sub-theme**	Resilience capabilities
Design principle	The organization shall develop and integrate resilience capabilities across the organization by fostering specific skills, allocating essential resources, and establishing robust processes that enable effective anticipation, response, and recovery from disruptions.		
Implementation guidance	▪ Evaluation of the current state of the organization's resilience capabilities by identifying strengths, weaknesses, and gaps. This assessment should be used to prioritize areas for development and improvement. ▪ Identification of the specific skills, resources, and processes that are critical to the organization's ability to anticipate, withstand, respond to, and recover from disruptions. These may include risk management, business continuity, crisis management, and adaptive capacity. ▪ Ensure that the necessary resources, including personnel, technology, and financial assets, are allocated to support the development and maintenance of resilience capabilities.		

Design principle: 6.4 Resilience capabilities	
	▪ Provide training programs and development opportunities to build the necessary skills and knowledge for resilience. This may include workshops, certifications, and simulations focused on risk management, business continuity, and crisis response. The objective should be to educate employees on resilience policies, procedures, and their roles in maintaining operational continuity. ▪ Establish and document processes for key resilience activities, such as risk assessments, incident response, and recovery planning. Ensure these processes are regularly reviewed and updated to reflect changing conditions and best practices. ▪ Utilize technology solutions to support resilience capabilities, such as risk management software, communication platforms, and data backup systems. Ensure that critical systems are secure, scalable, and capable of supporting resilience efforts. ▪ Encourage collaboration across different departments and functions to build a cohesive approach to resilience. Establish cross-functional teams to address resilience challenges and ensure a coordinated response to disruptions. ▪ Collaborate with external partners, such as suppliers, customers, and regulatory bodies, to enhance resilience capabilities. Ensure that these partners are aligned with the organization's resilience objectives and can support recovery efforts. ▪ Continuously monitor the effectiveness of resilience capabilities through regular assessments, performance reviews, and incident analysis. Use key performance indicators (KPIs) to track progress and identify areas for improvement. ▪ Regularly test and validate resilience capabilities through simulations, drills, and exercises. Use these tests to identify gaps and areas for enhancement, and update plans and processes accordingly. ▪ Promotion of a culture of continuous improvement by encouraging employees to proactively identify and report potential risks and areas for enhancement. The organization should foster a culture of resilience within the organization by encouraging proactive risk management, continuous learning, and adaptability.

Article mapping			
AI ACT Ref#	▪ Article 15.1 ▪ Article 15.4 ▪ Article 15.5	**GDPR Ref#**	▪ Article 32.1
NIS2 Ref#	▪ Article 20 ▪ Article 21	**DORA Ref#**	▪ Article 5.1 ▪ Article 5.2 ▪ Article 6.1 ▪ Article 9.2 ▪ Article 9.3 ▪ Article 11.2 ▪ Article 12.1

Design principle: 6.4 Resilience capabilities			
			▪ Article 12.2 ▪ Article 12.4 ▪ Article 12.5 ▪ Article 12.7 ▪ Article 13

4.6.5. Sub-theme: Resilience monitoring & assessment

Sub-theme definition: Resilience monitoring and assessment involve the continuous evaluation of an organization's ability to withstand, respond to, and recover from disruptions. This process includes tracking key performance indicators, conducting regular reviews, and identifying areas for improvement to ensure ongoing operational continuity and adaptability.

Design principle: 6.5 Resilience monitoring & assessment			
Theme	Continuity & resilience	**Sub-theme**	Resilience monitoring & assessment
Design principle	The organization shall establish a continuous monitoring and assessment framework to evaluate the organization's ability to withstand, respond to, and recover from disruptions.		
Implementation guidance	▪ Identification and definition of KPIs that are critical to measuring the organization's resilience. These indicators should cover various aspects such as response times, recovery times, system uptime, and incident frequency. ▪ Creation of a structured framework for continuous monitoring of resilience activities. This framework should include tools, processes, and responsibilities for tracking and reporting on resilience metrics. ▪ Implementation of monitoring tools such as monitoring software, dashboards, and alert systems to track resilience KPIs in real-time. Ensure these tools are integrated with existing systems for seamless data collection and analysis. ▪ Conduct and schedule regular assessments to evaluate the effectiveness of resilience strategies and plans. These assessments should include internal audits, risk assessments, and performance reviews. ▪ Regularly conduct simulations and drills to test the organization's response and recovery capabilities. Use these exercises to identify gaps and areas for improvement in resilience plans. ▪ Collect and analyze incident reports to understand the root causes of disruptions and the effectiveness of the response. Use this analysis to inform future resilience planning and improvements. ▪ Involving key stakeholders, including employees, management, and external partners, in the monitoring and assessment process. Ensure transparent communication of findings and encourage feedback for continuous improvement.		

Design principle: 6.5 Resilience monitoring & assessment			
	▪ Based on the insights gained from monitoring and assessments, regularly review and update resilience plans and strategies. Ensure that changes are documented and communicated to all relevant parties. ▪ Compare the organization's resilience performance against industry standards and best practices. Use benchmarking to identify areas where the organization can enhance its resilience capabilities. ▪ Provide regular reports on resilience monitoring and assessment findings to senior leadership. Ensure that leadership is informed of the organization's resilience status and any necessary actions to address identified issues.		
Article mapping			
AI ACT Ref#	▪ N/A	**GDPR Ref#**	▪ Article 32.1
NIS2 Ref#	▪ Article 21	**DORA Ref#**	▪ Article 10.1 ▪ Article 11.4 ▪ Article 11.6 ▪ Article 13.3 ▪ Article 13.5

4.7. Third-party management

Theme definition: Third-party management involves the systematic process of overseeing and controlling interactions and relationships with external entities that provide goods, services, or perform functions on behalf of an organization. It encompasses activities such as due diligence, risk assessment, contract management, and performance monitoring to ensure that third-party engagements align with the organization's objectives and compliance requirements.

Sub-themes:

- Third-party management governance & oversight
- Third-party management policy & procedures
- Third-party management lifecycle
- Third-party management reporting

4.7.1. Sub-theme: Third-party management governance & oversight

Sub-theme definition: Third-party management governance and oversight involve the structured framework and processes for overseeing and controlling interactions with external entities that provide goods, services, or perform functions on behalf of an organization. This ensures that third-party engagements align with the organization's objectives, mitigate risks, and comply with regulatory and contractual requirements.

Design principle: 7.1 Third-party management governance & oversight			
Theme	Third-party management	**Sub-theme**	Third-party management governance & oversight
Design principle	The organization shall establish a structured framework and processes for governance and oversight of third-party relationships to ensure alignment with organizational objectives, risk mitigation, and compliance with regulatory and contractual requirements.		
Implementation guidance	▪ Creation of a governance framework that outlines the principles, policies, and procedures for managing third-party relationships. Ensuring the framework aligns with the organization's strategic objectives, risk management practices, and regulatory requirements. ▪ Defining and assigning specific roles and responsibilities for governance and oversight of third-party management. Designation of a dedicated team or individual responsible for coordinating third-party management activities and ensuring accountability across the organization. ▪ Forming oversight committees or working groups that include representatives from key departments such as legal, compliance, procurement, and risk management. These committees should regularly review third-party management activities and provide strategic direction. ▪ Encouraging a culture of continuous improvement by regularly reviewing and updating third-party management governance and oversight practices. Staying informed about industry best practices and emerging trends to enhance the organization's third-party management capabilities. ▪ Promotion of open communication and collaboration between the organization and its third parties. Establishing clear communication channels and protocols for reporting issues, sharing information, and addressing concerns.		
Article mapping			
AI ACT Ref#	▪ Article 25.1	**GDPR Ref#**	▪ Article 28.1 ▪ Article 28.2 ▪ Article 28.3 ▪ Article 28.4
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ Article 28.1 ▪ Article 28.2

4.7.2. Sub-theme: Third-party management policy & procedures

Sub-theme definition: Third-party management policy and procedures are the formal guidelines and processes established by an organization to manage interactions and relationships with external entities that provide goods, services, or perform functions on its behalf. These policies and procedures ensure that third-party engagements are conducted in a manner that aligns with organizational objectives, mitigates risks, and complies with regulatory and contractual requirements.

Design principle: 7.2 Third-party management policy & procedures			
Theme	Third-party management	**Sub-theme**	Third-party management policy & procedures
Design principle	The organization shall develop and implement comprehensive policies and procedures to manage interactions and relationships with third parties, ensuring alignment with organizational objectives, risk mitigation, and compliance with regulatory and contractual requirements.		
Implementation guidance	▪ Development a comprehensive third-party management policy framework which clearly outlines the objectives and scope of the third-party management policy, ensuring alignment with the organization's strategic goals, risk management practices and regulatory requirements. ▪ Ensuring the policy is approved by the organizations management body and is communicated to all relevant stakeholders within or outside the organization. ▪ Development and documentation of standardized processes and procedures for each stage of the third-party management lifecycle, including selection, onboarding, monitoring, performance evaluation, and termination. It is important to ensure that third-party management processes are integrated with the organization's overall risk management framework. ▪ Ensuring the integration of third-party risk management into the organization's overall risk management framework. Risk assessment criteria and tools should be established to evaluate third-party risks consistently in line with organizations enterprise risk management criteria. ▪ Escalation procedures should be developed and implemented for addressing significant issues or breaches in third-party relationships, ensuring that issues are promptly reported to senior management and appropriate actions are taken.		
Article mapping			
AI ACT Ref#	▪ Article 25.4	**GDPR Ref#**	▪ Article 28.1 ▪ Article 28.2 ▪ Article 28.3 ▪ Article 28.4 ▪ Article 28.9
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ Article 28.1 ▪ Article 28.2

Design principle: 7.2 Third-party management policy & procedures			
			▪ Article 28.3 ▪ Article 28.4 ▪ Article 28.5 ▪ Article 28.6 ▪ Article 28.7 ▪ Article 28.8 ▪ Article 29.1 ▪ Article 29.2

4.7.3. Sub-theme: Third-party management lifecycle

Sub-theme definition: The third-party management lifecycle encompasses the end-to-end process of managing relationships with external entities, from initial selection and due diligence to ongoing monitoring, performance evaluation, and contract termination. This lifecycle ensures that third-party engagements are effectively controlled, risks are mitigated, and compliance with organizational and regulatory requirements is maintained throughout the relationship.

Design principle: 7.3 Third-party management lifecycle			
Theme	Third-party management	**Sub-theme**	Third-party management lifecycle
Design principle	The organization shall establish a comprehensive third-party management lifecycle that includes initial selection, due diligence, ongoing monitoring, performance evaluation, and contract termination to ensure effective control and oversight of third-party relationships.		
Implementation guidance	▪ Development a comprehensive lifecycle framework that outlines the stages of the third-party management lifecycle. This framework should align with the organization's strategic goals, risk management practices, and regulatory requirements. The lifecycle should include stages such as selection, onboarding, ongoing monitoring, performance evaluation, and termination. ▪ Develop and integrate specific skills, resources, and processes to effectively oversee and control interactions with third parties by identifying key capabilities, assigning roles & responsibilities for third-party management activities and conducting relevant training and development programs. ▪ Establishment of clear criteria for selecting third parties, including financial stability, compliance history, reputation, and alignment with organizational values and regulatory requirements. ▪ Implementation of a rigorous due diligence process using standardized checklists and assessment tools to evaluate potential third parties. This assessment should cover factors such as legal and regulatory compliance, cybersecurity practices, and operational capabilities. The selection and due diligence findings should be reviewed and approved by relevant stakeholders, including legal, compliance, and risk management teams.		

Design principle: 7.3 Third-party management lifecycle			
	▪ Creation of standardized onboarding procedures to ensure that third parties understand and agree to the organization's expectations and requirements. This includes providing training on relevant policies, procedures, and compliance obligations. ▪ Developing and executing of standardized contractual agreement, clearly defining the terms and conditions of third-party engagements. These contracts should include provisions for performance expectations, compliance requirements, risk management, data protection, and termination clauses. Additionally, these contracts should be in line with regulatory requirements. ▪ Mechanisms for ongoing monitoring of third-party performance, compliance, and risk status should be established. Key performance indicators (KPIs), regular audits, and performance reviews should be used to track and evaluate third-party activities. ▪ Regular reviewing and assessing of third-party performance against established KPIs and contractual obligations should be conducted. Areas for improvement should be identified, and corrective actions should be taken as needed. Feedback mechanisms should be established to gather input from third parties and internal stakeholders on the effectiveness of the third-party relationship. ▪ Creating and conducting a standardized procedure for terminating third-party relationships, including criteria for termination and steps for offboarding. Termination processes should be conducted in a manner that minimizes disruption to the organization and protects its interests. All organizational data and assets should be securely returned or destroyed as part of the offboarding process, and access to systems and information should be revoked. A post-termination review should be conducted to assess the reasons for termination and identify any lessons learned, using this information to improve future third-party management practices. ▪ Detailed documentation of all third-party management activities, including due diligence assessments, contractual agreements, performance evaluations, and audit reports, should be maintained. Documentation should be easily accessible and support transparency and accountability. An audit trail of third-party management activities should be kept to facilitate audits and reviews, ensuring that records are retained in accordance with regulatory and organizational requirements. ▪ Regularly reviewing and updating the third-party management lifecycle framework and processes to ensure they remain relevant and effective. Feedback from stakeholders and lessons learned from past experiences should be incorporated. Staying informed about industry best practices, emerging trends, and regulatory changes is crucial for continuously enhancing third-party management capabilities.		
Article mapping			
AI ACT Ref#	▪ Article 25.4	**GDPR Ref#**	▪ Article 28.1 ▪ Article 28.3 ▪ Article 28.4

Design principle: 7.3 Third-party management lifecycle			
NIS2 Ref#	▪ Article 21.2 ▪ Article 21.3	**DORA Ref#**	▪ Article 28.1 ▪ Article 28.4 ▪ Article 28.7 ▪ Article 28.8 ▪ Article 29.1 ▪ Article 30.2 ▪ Article 30.3

4.7.4. Sub-theme: Third-party management reporting

Sub-theme definition: Third-party management reporting involves the systematic process of documenting and communicating the performance, compliance, and risk status of external entities that provide goods, services, or perform functions on behalf of an organization. This reporting ensures transparency, supports informed decision-making, and helps maintain accountability in third-party relationships.

Design principle: 7.4 Third-party management reporting			
Theme	Third-party Management	**Sub-theme**	Third-party management reporting
Design principle	The organization shall establish a systematic process for documenting and communicating the performance, compliance, and risk status of third-party relationships to ensure transparency and informed decision-making.		
Implementation guidance	▪ Developing a comprehensive reporting framework that clearly outlines the objectives and scope of third-party management reporting. This framework should ensure alignment with the organization's strategic goals and risk management practices. ▪ Identification and definition of key performance indicators (KPIs) that are critical to measuring third-party performance, compliance, and risk status. Relevant KPIs may include service delivery metrics, compliance adherence, financial stability, and incident reports. Performance targets and benchmarks should be set for each KPI to evaluate third-party performance against organizational standards. ▪ Standardized reporting requirements for third parties should be established, specifying the type of information to be reported, the frequency of reporting, and the format in which reports should be submitted. When defining standardized reporting regulatory requirements should be taken into account. ▪ Clear reporting procedures should be established, including specific timelines for third-party reporting. This includes defining the frequency of reports (e.g., monthly, quarterly) and deadlines for submission. Responsibilities for preparing, reviewing, and submitting reports should be clearly assigned within both the organization and third-party entities.		

Design principle: 7.4 Third-party management reporting	
	▪ Regular monitoring of third-party compliance with regulatory and contractual requirements should be conducted, including periodic compliance audits and reviews. ▪ Summary reports that consolidate key findings from third-party reports should be prepared and communicated to management body and relevant stakeholders. These summaries should be clear, concise, and actionable, providing insights and recommendations for addressing any issues or areas for improvement. ▪ Criteria for escalating significant issues or breaches identified in third-party reports should be established. Clear escalation paths and responsibilities should be defined to ensure timely resolution of issues, with significant issues promptly reported to senior management and appropriate actions taken. ▪ Conducting tegular training programs for employees involved in third-party management reporting to ensure they understand the reporting framework, procedures, and their roles in the process. Additionally, guidance and support should be provided to third parties to help them understand reporting requirements and improve the quality of their reports. ▪ Maintaining detailed records of all third-party reporting activities including submitted reports, review findings, and actions taken. Documentation should be easily accessible and support transparency and accountability. An audit trail of reporting activities should also be maintained to facilitate audits and reviews. ▪ Regularly reviewing and updating the third-party management reporting framework and procedures to ensure they remain relevant and effective. Feedback from both internal stakeholders and third parties should be encouraged to identify areas for improvement and enhance the reporting process. Staying informed about industry best practices and emerging trends is crucial for continuously enhancing third-party management reporting capabilities.

Article mapping			
AI ACT Ref#	▪ N/A	**GDPR Ref#**	▪ N/A
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ Article 28.3 ▪ Article 28.4 ▪ Article 28.5 ▪ Article 28.6 ▪ Article 29.1 ▪ Article 29.2

4.8. Data protection & privacy

Theme definition: Data protection and privacy are focused on ensuring that personal and sensitive information is handled securely and in compliance with legal standards, safeguarding the rights and freedoms of individuals.

Sub-themes:

- Data protection & privacy principles
- Data sharing
- Privacy by design

4.8.1. Sub-theme: Data protection & privacy principles

Sub-theme definition: Data protection and privacy principles encompass the foundational guidelines and practices that govern the collection, processing, storage, and sharing of personal and sensitive data. These principles are designed to uphold the integrity and confidentiality of data, ensure its lawful and fair handling, and protect the rights of individuals by enforcing transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.

Design principle: 8.1 Data protection & privacy principles			
Theme	Data protection & privacy	**Sub-theme**	Data protection & privacy principles
Design principle	The organization shall integrate privacy and data protection principles into all aspects of its operations that process personal data, particularly within its critical business infrastructure and AI systems where personal data is processed. The principles to be embedded are as follows: ▪ Lawfulness, fairness, and transparency ▪ Purpose limitation ▪ Data accuracy ▪ Storage limitation ▪ Data minimization ▪ Confidentiality and integrity		
Implementation guidance	Data protection and privacy shall be foundational elements in the design and operation of all systems, assets, processes and procedures where personal data is handled, ensuring adherence to core data protection and privacy principles. As such, organizations shall: ▪ Ensure a valid legal basis for processing personal data is in place and process this personal data in a manner that individual's rights are not negatively impacted. ▪ Create comprehensive privacy policies and procedures, that outline the organization's data handling practices. ▪ Collect personal data to a minimum and only necessary for specified purposes ▪ Regularly review data collection practices, and maintain data accuracy by providing mechanisms for individuals to update or correct their information. ▪ Regularly perform data protection impact assessments (DPIAs) to identify and mitigate privacy risks associated with data processing activities, and integrate findings into data handling processes. ▪ Deploy robust technical and organizational measures to protect personal data, establish clear data retention policies, and ensure secure disposal of data that is no longer needed.		
Article mapping			
AI ACT Ref#	▪ Article 10.5 ▪ Article 13 ▪ Article 50.1	**GDPR Ref#**	▪ Article 5.1 ▪ Article 6.1 ▪ Article 7

Design principle: 8.1 Data protection & privacy principles			
	▪ Article 50.2 ▪ Article 50.3 ▪ Article 50.4 ▪ Article 50.5 ▪ Article 50.6 ▪ Article 59 ▪ Article 60.4 ▪ Article 60.5 ▪ Article 61		▪ Article 25.1 ▪ Article 25.2 ▪ Article 32.1 ▪ Article 32.2 ▪ Article 35.1 ▪ Article 35.3 ▪ Article 35.7
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ N/A

4.8.2. Sub-theme: Data sharing

Sub-theme definition: Data sharing covers the protocols and procedures for the secure and compliant exchange of information between entities, ensuring that data handling meets transparency, accountability, and privacy and data protection standards.

Design principle: 8.2 Data sharing			
Theme	Data protection & privacy	**Sub-theme**	Data sharing
Design principle	Organizations shall establish and maintain robust mechanisms for data sharing with third parties, in line with legal obligations. This involves implementing technical and organizational measures to protect data during transfer, ensuring legal compliance for data transfers, and maintaining transparency and accountability about data-sharing practices. Organizations shall document data-sharing processes and perform continuous monitoring and risk management to prevent unauthorized access and data breaches.		
Implementation guidance	Data sharing, both internally within the organization as well as with third parties, shall be conducted in a secure manner, ensuring that personal and sensitive data are safeguarded throughout the entire transfer process, including during intraorganizational exchanges. This approach upholds transparency, accountability, and protection standards across all data sharing activities. ▪ Create comprehensive data sharing policies that outline the protocols and procedures for both internal and external data sharing. ▪ Ensure policies cover the secure handling of personal and sensitive data throughout the entire transfer process, including intraorganizational exchanges. ▪ Implement secure data transfer mechanisms and ensure that all data-sharing is conducted on the basis of valid agreements and contracts with third parties.		

Design principle: 8.2 Data sharing			
Article mapping			
AI ACT Ref#	▪ Article 11.1 ▪ Article 12 ▪ Article 13 ▪ Article 53.1 ▪ Article 53.2 ▪ Article 55.1 ▪ Article 55.3	**GDPR Ref#**	▪ Article 20 ▪ Article 25.1 ▪ Article 25.2 ▪ Article 45.1 ▪ Article 46.1 ▪ Article 46.2 ▪ Article 46.3 ▪ Article 47.2
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ N/A

4.8.3. Sub-theme: Privacy by design

Sub-theme definition: Privacy by Design is an approach that integrates privacy and data protection principles into the design and development of systems, processes, and products from the outset. It ensures that privacy considerations are proactively embedded into every aspect of an organization's operations, rather than being an afterthought. This approach upholds the principles of transparency, accountability, and user control, fostering digital trust by ensuring that personal and sensitive data are handled securely, lawfully, and ethically throughout their lifecycle.

Design Principle: 8.3 Privacy by design			
Theme	Data protection & privacy	**Sub-theme**	Privacy by design
Design principle	Organizations shall integrate privacy considerations into the design and operation of their systems and processes from the outset. This involves implementing data protection measures that are proactive rather than reactive, ensuring that personal data is processed with the highest level of privacy and security. Organizations shall conduct privacy impact assessments to identify and mitigate risks associated with data processing activities, and ensure that data minimization principles are adhered to by limiting the collection and retention of personal data to what is necessary for the intended purpose.		
Implementation guidance	Data management practices shall uphold privacy by design principles and be robust and systematic, ensuring the accuracy, security, availability, and integrity of personal data across all processes, products and services. These practices must align with regulatory requirements to guarantee data reliability, operational efficiency, and compliance. As such, organization shall: ▪ Promote a culture of privacy awareness and responsibility within the organization through regular training and awareness programs. ▪ Integrate privacy and data protection features into the initial design and architecture of IT systems, applications, and business processes.		

Design Principle: 8.3 Privacy by design			
	▪ Conduct privacy impact assessments (PIAs) during the development phase of processes, products and services to identify and mitigate potential privacy risks. ▪ Minimize data collection and processing to only what is necessary for the specified purpose.		
Article mapping			
AI ACT Ref#	▪ N/A	**GDPR Ref#**	▪ Article 25.1 ▪ Article 25.2 ▪ Article 25.3 ▪ Article 35.1 ▪ Article 35.3 ▪ Article 35.7
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ N/A

4.9. Rights & ethics

Theme definition: Rights & ethics refers to the importance of protecting individuals' legal entitlements to privacy and data security while ensuring that security practices are conducted with integrity and fairness. This combination ensures that security measures not only comply with legal standards but also adhere to moral principles that respect and uphold individuals' rights and trust.

Sub-themes:

- Ethical oversight
- Complaints and requests
- Informed consent & transparency

4.9.1. Sub-theme: Ethical oversight

Sub-theme Definition: An ethical framework aims to contribute to the development and deployment of safe and reliable data-driven applications, providing organizations with the tools to assess the ethical aspects of their AI applications and ensuring consumers have the trust and confidence in the use of AI.

Design principle: 9.1 Ethical oversight			
Theme	Rights & ethics	**Sub-theme**	Ethical oversight
Design principle	Organizations shall establish clear accountability and governance structures to oversee the ethical use of data and technology. It includes the development of policies, procedures, and oversight mechanisms to ensure that organizations adhere to ethical standards and legal requirements. It shall also address the need for regular audits, assessments, and reporting to maintain transparency and accountability, thereby fostering trust among stakeholders.		

Design principle: 9.1 Ethical oversight			
Implementation guidance	▪ Establish a cross-functional ethics committee or board with representatives from key departments, including legal, compliance, IT, and human resources. ▪ Develop a comprehensive ethical oversight framework that includes policies, procedures, and guidelines for the ethical use of data and technology. ▪ Implement a robust audit and assessment program to regularly evaluate compliance with ethical standards and identify areas for improvement. ▪ Create transparent reporting mechanisms to communicate ethical practices and incidents to stakeholders, ensuring accountability and trust. ▪ Provide regular training and awareness programs for employees to reinforce the importance of ethical oversight and responsible data and technology use (including code of conduct).		
Article mapping			
AI ACT Ref#	▪ Article 8 ▪ Article 14 ▪ Article 17.1	**GDPR Ref#**	▪ Article 22.3
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ N/A

4.9.2. Sub-theme: Complaints and requests

Sub-theme definition: Complaints and requests pertain to the mechanisms and processes consumers can use to exercise their rights, such as accessing personal information, requesting corrections of data related to them, or lodging complaints regarding privacy violations, unethical responses, unfair practices or other harmful occurrences, ensuring these processes are accessible, transparent, and effective.

Design principle: 9.2 Complaints and requests			
Theme	Rights & ethics	**Sub-Theme**	Complaints & requests
Design principle	Organizations shall design and implement sufficient mechanisms and processes to protect the fundamental rights of individuals, including the ability for individuals to exercise their rights and to lodge complaints.		

Implementation guidance	▪ Organizations shall have sufficient mechanisms and processes in place to ensure the following rights of individuals:
	  ▪ To obtain confirmation whether their personal data is being processed;
	  ▪ To rectify incorrect personal data regarding them;
	  ▪ To erase the personal data regarding them;
	  ▪ To restrict the processing of their personal data;		

Design principle: 9.2 Complaints and requests			
	▪ To receive their personal data which is processed by the organization; ▪ Object to processing of their personal data; ▪ To have a human oversight in the automated decision making processes concerning their personal situation. ▪ Organizations shall provide individuals with the ability to lodge complaints and file requests regarding the abovementioned rights. ▪ Organizations shall perform prior assessments to determine whether their data processing activities potentially infringe on individuals' fundamental rights (data protection impact assessment) or whether the introduction of high-risk AI systems does so (fundamental rights impact assessment). If a data protection impact assessment has already been performed, the fundamental rights impact assessment shall complement this assessment.		
Article mapping			
AI ACT Ref#	▪ Article 85	**GDPR Ref#**	▪ Article 12 ▪ Article 13 ▪ Article 14 ▪ Article 15 ▪ Article 16 ▪ Article 17 ▪ Article 18 ▪ Article 19 ▪ Article 20 ▪ Article 21 ▪ Article 22
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ N/A

4.9.3. Sub-theme: Informed consent & transparency

Sub-theme definition: Organizations shall obtain explicit and informed consent from individuals before collecting, using, or sharing their personal data. It highlights the need for transparency in how data is handled, ensuring that individuals are fully aware of what data is being collected, for what purpose, and how it will be used. This builds trust by ensuring that individuals have control over their own information and are not subjected to hidden or deceptive practices.

Design principle: 9.3 Informed consent & transparency			
Theme	Rights & ethics	**Sub-theme**	Informed consent & transparency
Design principle	Organizations shall ensure sufficient communication with the individuals they interact with by disclosing, prior to and during the relationship, information about the relevant processes and systems, or in the case of any significant updates or events.		
Implementation guidance	▪ Publish thorough and easily accessible privacy notices, written in clear language for transparency. ▪ Update privacy policies and procedures that align with informed consent and transparency principles. ▪ Train employees on the importance of informed consent and transparency, and provide them with the tools and knowledge to uphold these principles in their daily work. ▪ Engage with stakeholders, including customers, regulators, and industry bodies, to continuously improve and uphold informed consent and transparency practices. ▪ In case of automated decision making, organizations must provide meaningful information about the logic involved in the decision-making process, as well as the significance and consequences of such processing for the individual(s). ▪ In case of providing AI systems to the market, organizations shall ensure that their users are sufficiently informed that they are interacting with an AI system, the AI system delivers a specific level of accuracy and there is a human oversight of the AI system. Furthermore, organizations shall be sufficiently transparent regarding the operation of their AI systems so that their users could interpret the systems' output and use it appropriately.		
Article mapping			
AI ACT Ref#	▪ Article 11.1 ▪ Article 12 ▪ Article 12.1 ▪ Article 12.2 ▪ Article 12.3 ▪ Article 13 ▪ Article 13.1 ▪ Article 13.2	**GDPR Ref#**	▪ Article 12.1 ▪ Article 12.3 ▪ Article 12.4 ▪ Article 12.7 ▪ Article 13.1 ▪ Article 13.2 ▪ Article 14.1 ▪ Article 14.2

Design principle: 9.3 Informed consent & transparency			
	▪ Article 13.3 ▪ Article 50 ▪ Article 52.1 ▪ Article 52.2 ▪ Article 86		▪ Article 19
NIS2 Ref#	▪ N/A	**DORA Ref#**	▪ N/A

4.10. Incident management

Theme definition: Incident management is the process of identifying, responding to, and resolving incidents that disrupt normal operations, with the goal of minimizing impact and restoring services as quickly as possible. It involves coordinated efforts to detect, analyze, and mitigate incidents, followed by post-incident reviews to prevent recurrence and improve future response strategies.

Sub-themes:

- Incident identification & classification
- Incident response
- Incident notification & reporting
- Post incident & lessons learned

4.10.1. Sub-theme: Incident identification & classification

Sub-theme definition: Incident identification and classification involve the systematic process of detecting and categorizing incidents based on their nature, severity, and impact on the organization. This process enables prompt and appropriate response actions, ensuring that incidents are managed effectively to minimize disruption and mitigate risks.

Design principle: 10.1 Incident identification & classification			
Theme	Incident management	**Sub-theme**	Incident identification & classification
Design principle	Establishment of a systematic process for detecting and categorizing incidents based on their nature, severity, and impact, ensuring prompt and appropriate response actions.		
Implementation guidance	▪ Creation of a comprehensive incident management policy that outlines the objectives, scope, and principles for incident identification and classification. Ensuring the policy aligns with the organization's overall risk management and compliance frameworks. ▪ Establishment of clear categories, severity levels and criteria for incidents based on their nature, impact, urgency and taking into account regulatory requirements. ▪ Creation of detailed guidelines for classifying incidents based on predefined categories and severity levels. Include examples and		

Design principle: 10.1 Incident identification & classification	
	scenarios to help employees and the incident response team accurately classify incidents. ▪ Categorization of incidents according to relevant regulatory frameworks (e.g., AI Act, GDPR, NIS2, DORA) to ensure clarity from the outset regarding the applicable regulatory reporting obligations that must be followed for each incident. ▪ Deployment of tools and technologies to detect incidents in real-time. This may include monitoring systems, early warning indicators, intrusion detection systems, automated alerts, and reporting mechanisms to ensure timely identification of incidents. ▪ Creation of standardized procedures for reporting incidents, including clear guidelines on how, when, and to whom incidents should be reported. Ensuring that all employees are aware of these procedures and understand their role in the incident reporting process. ▪ Providing training to employees on incident identification and classification processes. Ensuring they understand the importance of timely and accurate reporting, and how to use the tools and procedures in place. ▪ Usage of a centralized incident management system to log, track, and manage incidents from identification to resolution. Ensuring that the system supports incident classification and provides visibility into incident status and trends. ▪ Regularly conducting drills and simulations to test the incident identification and classification processes. Use these exercises to identify gaps, improve procedures, and ensure readiness for real incidents. ▪ Continuously monitor the effectiveness of incident identification and classification processes. Conduct regular reviews and audits to ensure compliance with policies and procedures, and make necessary adjustments based on lessons learned and evolving risks.

Article mapping			
AI ACT Ref#	▪ Article 73.2 ▪ Article 73.6	**GDPR Ref#**	▪ Article 33.3
NIS2 Ref#	▪ Article 21.2 ▪ Article 23.3	**DORA Ref#**	▪ Article 10.1 ▪ Article 10.2 ▪ Article 17 ▪ Article 18.1 ▪ Article 18.2 ▪ Article 19.1

4.10.2. Sub-theme: Incident response

Sub-theme definition: Incident response is the structured process of identifying, managing, and resolving incidents that disrupt normal operations, with the goal of minimizing impact and restoring services as quickly as possible. It involves coordinated efforts to detect, assess, contain, eradicate, and recover from incidents, followed by post-incident analysis to improve future response strategies.

Design principle: 10.2 Incident response			
Theme	Incident management	**Sub-theme**	Incident response
Design principle	Establishment of a structured and coordinated incident response process to effectively identify, manage, and resolve incidents, minimizing impact and ensuring rapid restoration of services.		
Implementation guidance	▪ Creation of a comprehensive incident response policy that outlines the objectives, scope, and principles for managing incidents. Ensuring the policy aligns with the organization's overall risk management and compliance frameworks. ▪ Establishment of dedicated incident response teams composed of individuals with the necessary skills and expertise to handle incidents. Define roles and responsibilities for each team member, including incident coordinators, technical experts, and communication leads. ▪ Development of detailed incident response plans that provides step-by-step procedures for responding to different types of incidents. The plan should include incident detection, assessment, containment, eradication, recovery, and post-incident review phases. ▪ Development of standardized templates for incident reports to ensure consistent and comprehensive documentation for internal and external purposes (e.g., reporting towards regulators). Include fields for key information such as incident description, date and time, affected systems, impact assessment, actions taken and ensure alignment with regulatory requirements. ▪ Providing regular training and awareness programs for employees on incident response procedures. Ensure that all staff, including the incident response team, are familiar with the incident response plan and their specific roles during an incident. ▪ Regularly conduct drills and simulations to test the incident response plan and the readiness of the incident response team. Use these exercises to identify gaps, improve procedures, and ensure preparedness for real incidents. ▪ Continuously monitor the effectiveness of the incident response process. Conduct regular reviews and audits to ensure compliance with policies and procedures, and make necessary adjustments based on lessons learned and evolving risks.		
Article mapping			
AI ACT Ref#	▪ Article 17.1 ▪ Article 20	**GDPR Ref#**	▪ Article 32.1 ▪ Article 33

Design principle: 10.2 Incident response			
	▪ Article 26.5 ▪ Article 55.1 ▪ Article 62.1 ▪ Article 62.2 ▪ Article 62.3 ▪ Article 73		▪ Article 34
NIS2 Ref#	▪ Article 21.1 ▪ Article 21.2 ▪ Article 23.1 ▪ Article 23.2 ▪ Article 23.3 ▪ Article 23.4 ▪ Article 30.1	**DORA Ref#**	▪ Article 10.1 ▪ Article 10.2 ▪ Article 11.2 ▪ Article 11.10 ▪ Article 12.7 ▪ Article 14.1 ▪ Article 17 ▪ Article 18.1 ▪ Article 18.2 ▪ Article 19.1 ▪ Article 19.2 ▪ Article 19.3 ▪ Article 19.4

4.10.3. Sub-theme: Incident notification & reporting

Sub-theme definition: Incident notification and reporting involve the systematic process of promptly informing relevant stakeholders about the occurrence of an incident and documenting the details for further analysis and response. This process ensures timely communication, facilitates coordinated response efforts, and supports compliance with regulatory and organizational requirements.

Design principle: 10.3 Incident notification & reporting			
Theme	Incident management	**Sub-theme**	Incident notification & reporting
Design principle	Establishment of a systematic process for prompt incident notification and reporting to ensure timely communication with relevant stakeholders and accurate documentation of incident details.		
Implementation guidance	▪ Creation of a comprehensive policy that outlines the objectives, scope, and principles for incident notification and reporting. Ensure the policy aligns with the organization's overall incident management framework and regulatory requirements. ▪ Establishment of clear procedures for incident notification and reporting, including specific steps for identifying, documenting, and communicating		

Design principle: 10.3 Incident notification & reporting			
	incidents. Ensure these procedures cover all types of incidents and are easily accessible to all employees. ▪ Determining the key stakeholders who need to be notified in the event of an incident, including internal teams (e.g., IT, security, management) and external parties (e.g., regulators, customers, partners). Creation of a contact list with up-to-date information for each stakeholder. ▪ Defining specific timelines for incident notification to ensure prompt communication. Establishment criteria for different types of incidents, specifying the urgency and required response times for notifying stakeholders. ▪ Defining clear escalation paths for incidents based on their severity and impact. Ensure that incidents are promptly escalated to the appropriate level of management and relevant stakeholders for timely response and decision-making. ▪ Establishment of multiple reporting channels for incidents, such as dedicated email addresses, hotlines, and online reporting forms. Ensuring these channels are easily accessible and well-publicized within the organization. ▪ Providing training to all employees on the incident notification and reporting procedures. Ensuring they understand the importance of timely reporting, how to use the reporting channels, and their role in the process. ▪ Continuously monitor the effectiveness of the incident notification and reporting process. Conduct regular reviews and audits to ensure compliance with policies and procedures, and make necessary adjustments based on lessons learned.		
Article mapping			
AI ACT Ref#	▪ Article 26.5 ▪ Article 55.1 ▪ Article 60.7 ▪ Article 73	**GDPR Ref#**	▪ Article 33 ▪ Article 34
NIS2 Ref#	▪ Article 23.1 ▪ Article 23.2 ▪ Article 23.3 ▪ Article 23.4 ▪ Article 30.1	**DORA Ref#**	▪ Article 11.10 ▪ Article 14.1 ▪ Article 19.1 ▪ Article 19.2 ▪ Article 19.3 ▪ Article 19.4

4.10.4. Sub-theme: Post incident & lessons learned

Sub-theme definition: Post-incident and lessons learned refer to the systematic process of reviewing and analyzing incidents after they have been resolved to identify root causes, evaluate response effectiveness, and capture actionable insights. This process aims to improve future incident management, enhance organizational resilience, and foster a culture of continuous improvement.

Design principle: 10.4 Post incident & lessons learned			
Theme	Incident management	**Sub-theme**	Post incident & lessons learned
Design principle	Organizations shall establish a structured process for conducting post-incident reviews and capturing lessons learned to identify root causes, evaluate response effectiveness, and implement improvements.		
Implementation guidance	▪ Creation of a comprehensive policy that outlines the objectives, scope, and principles for conducting post-incident reviews and capturing lessons learned. Ensuring the policy aligns with the organization's overall incident management framework and continuous improvement goals. ▪ Defining a structured process for conducting post-incident reviews, including specific steps for gathering information, analyzing the incident, and identifying lessons learned. Ensuring the process is documented and accessible to all relevant stakeholders. ▪ Assembly of a dedicated review team composed of individuals with the necessary expertise and knowledge to conduct thorough post-incident reviews. Including representatives from relevant departments, such as IT, security, operations, and management. ▪ Conducting post-incident reviews promptly after an incident has been resolved to ensure that information is fresh and accurate. Scheduling reviews within a specific timeframe, such as within one week of incident resolution. ▪ Collection of detailed information about the incident, including incident reports, logs, timelines, impact assessments, and response actions taken. Ensuring that all relevant data is gathered to provide a complete picture of the incident. ▪ Conducting a thorough analysis of the incident to identify the root cause, contributing factors, and the effectiveness of the response. ▪ Documenting key lessons learned from the incident, including what went well, what could have been done better, and any gaps or weaknesses in the incident response process. ▪ Based on the lessons learned, development of specific improvement actions to address identified gaps and enhance the organization's incident management capabilities. Assign responsibilities and set timelines for implementing these actions. ▪ Tracking the progress of improvement actions to ensure they are implemented effectively and within the specified timelines. Monitor the impact of these actions on the organization's incident management capabilities.		

Design principle: 10.4 Post incident & lessons learned			
	▪ Sharing the findings and lessons learned from the post-incident review with relevant stakeholders, including management, response teams, and affected departments. Ensure transparent communication to promote awareness and accountability. ▪ Incorporation of the lessons learned into the organization's policies, procedures, and incident response plans. Ensuring that updates are documented, communicated, and integrated into training programs. ▪ Encouraging a culture of continuous improvement by regularly conducting post-incident reviews and capturing lessons learned. Recognize and reward individuals and teams who contribute to the organization's learning and improvement efforts.		
Article mapping			
AI ACT Ref#	▪ N/A	**GDPR Ref#**	▪ N/A
NIS2 Ref#	▪ Article 21.2 ▪ Article 23.4	**DORA Ref#**	▪ Artikel 6.5 ▪ Article 13 ▪ Article 19.4

Appendix

Definitions

Accountability Framework:	Structured system that outlines the policies, procedures, roles, and responsibilities to ensure that an organization's activities are conducted transparently, ethically, and in alignment with its objectives.
Adaptive Capacity	Refers to an organization's ability to adjust and modify its processes and operations in response to disruptions or changes.
Applicability Assessment	The process that organizations use to determine which regulatory requirements are relevant to them and which are not. This assessment evaluates factors such as the type of organization, the sector in which it operates, and the nature of the services or products provided.
Digital Trust	Digital trust refers to the confidence that stakeholders have in an organization's ability to protect data, ensure privacy, and maintain security in digital interactions following regulatory requirements in the digital space.
Management Body	The management body is the group of individuals responsible for the governance and oversight of the organization. This may include the board of directors, executive management, or other designated leaders who are accountable for strategic decision-making and compliance.
Resilience Framework	A comprehensive system that ensures an organization's ability to anticipate, withstand, respond to, and recover from disruptions.
Risk Appetite	The level of risk an organization is willing to accept in pursuit of its objectives.
Risk Tolerance	Refers to the acceptable level of variation in performance related to specific risks. It defines the thresholds or limits for individual risks that the organization is willing to tolerate while still pursuing its objectives.

Acronyms

AI	Artificial Intelligence
BIA	Business Impact Analysis
DORA	Digital Operational Resilience Act
EDR	Endpoint Detection and Response
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
KRI	Key Risk Indicator
MFA	Multi-Factor Authentication
MVO	Minimum Viable Organization
NIS2	Network and Information Systems Directive 2
PIA	Privacy Impact Assessment
RBAC	Role-Based Access Control
SIEM	Security Information and Event Management
SWOT	Strengths, Weaknesses, Opportunities, Threats
UDDM	Unified Digital Management Model
VPN	Virtual Private Network

Contributors

Lead Authors*

- Rudrani Djwalapersad, EY Partner
- Sanne Fransen, EY Senior Manager
- Tim Leerdam, EY Senior Manager

Acknowledgements

This Unified Digital Management Model was co-created with valuable input and feedback from several key contributors from the Online Trust Coalition. They shared insights and lessons learned during various virtual and in-person sessions and consultations.

- Tom Vreeburg
- Joko Tenthof van Noorden
- Jorg Voeten
- Dwayne Valkenburg

Finally, special thanks are extended to Giulio, Bernadette, Bart, Babeth, Vanessa, Rosa, and Kirill from EY for their valuable contributions throughout the creation of the Unified Digital Management Model.

*All EY authors are part of EY Adviseurs B.V.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fuelled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 004070-25Gbl
ED None

ey.com