Charter
of Trust

Security by Default in view of major Cybersecurity Regulations

Publication date: 13.02.2025

Charter of Trust – Principle 3
Classification CoT Public

Executive Summary

In today's digitized world, cybersecurity plays a pivotal role in maintaining global stability, economic resilience, and individual privacy. Various regulations have been implemented to safeguard individuals, businesses, and infrastructure from the ever-evolving cyber threats. Each regulation mentioned in this document, though varying in scope and focus by region, aims to protect against potential breaches, data leaks, and other malicious activities that could disrupt operations and compromise sensitive information.

The principle of Security by Default, as advocated by the Charter of Trust, provides a universal standard for organizations to meet compliance requirements effectively. By embedding security measures from the outset, organizations can ensure compliance with regulations, foster trust with customers, safeguard their operations, and strengthen their market position. This approach not only helps organizations meet their legal obligations but also enhances their reputation and competitive advantage.

However, this publication has shown that regulators worldwide have taken different approaches to pursue common cybersecurity goals, leading to varied and sometimes conflicting regulatory frameworks. This complexity can make it challenging for organizations to navigate the cybersecurity landscape and ensure compliance with all relevant regulations.

Albeit not claiming to be exhaustive, this document serves as a roadmap to better navigate this complex landscape, thereby highlighting the benefits of aligning current cybersecurity regulations worldwide.[1] It supports the Charter of Trust's mission to create a secure digital environment for innovation. By using the guidelines outlined in this document, organizations can effectively manage their cybersecurity risks, protect their assets, and contribute to a more secure digital world.

[1] See also the Charter of Trust publication on Harmonization of Regulation - A Charter of Trust perspective.

Table of Contents

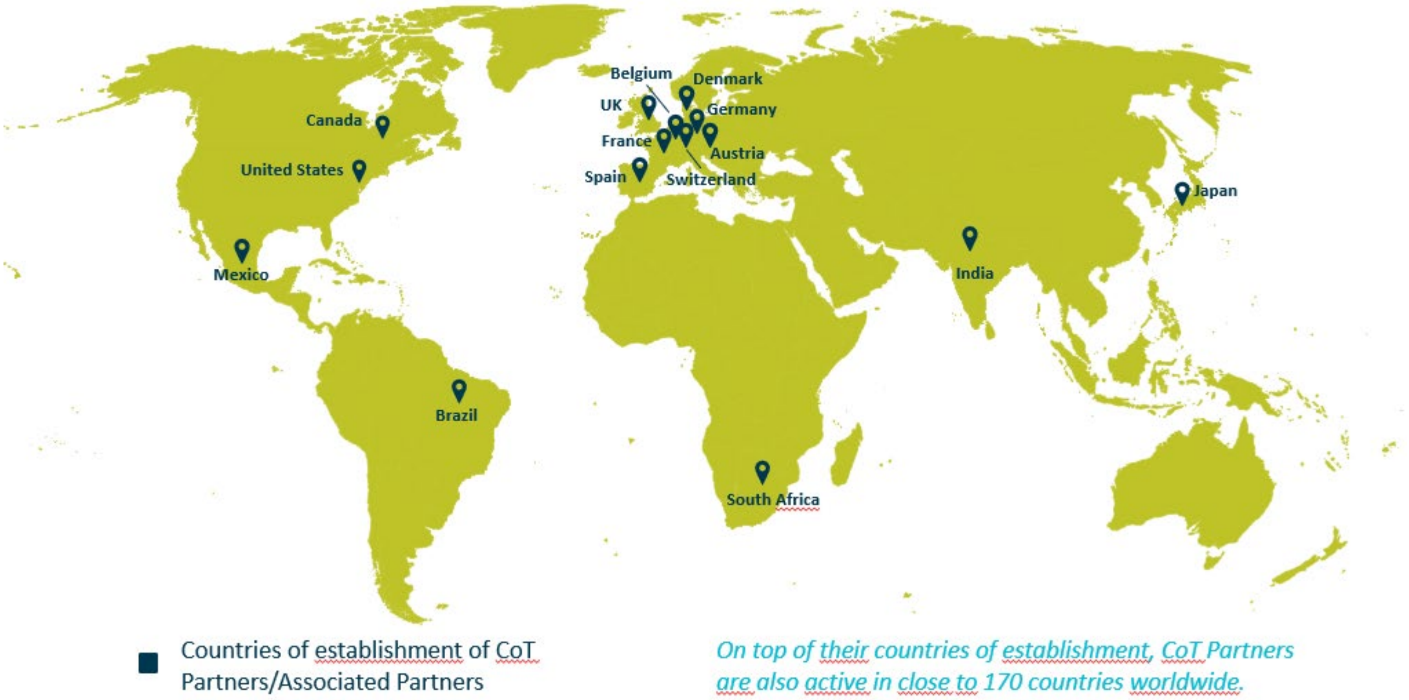
About the Charter of Trust

On February 16, 2018, the cornerstone for the Charter of Trust (CoT) was laid at the Munich Security Conference to enhance cybersecurity efforts and foster digital trust in the face of an increasingly complex and severe cyber threat landscape. The CoT is a non-profit alliance of leading global companies and organizations working across sectors to make the digital world of tomorrow a safer place. Our 13 Partners and 17 Associated Partners are operating in close to 170 countries on 5 continents in a diverse range of sectors. Altogether, CoT partners represent 1.8 million employees worldwide.

A continuously evolving group of members and partners has signed off on this cybersecurity initiative by endorsing its 10 fundamental principles, which foster three important objectives:

- To protect the data of individuals and companies
- To prevent damage to people, companies, and infrastructure
- To create a reliable foundation on which confidence in a networked, digital world can take root and grow.

Based on these principles fundamental to a secure digital world, the Charter of Trust is working to protect our increasingly digitized world and build a reliable foundation on which trust and digital innovation can flourish. It contributes to the development of effective cybersecurity policies that strengthen the global cybersecurity posture and it provides expertise on topics including AI, security by default, supply chain security, and education. This guideline is a Charter of Trust publication from the Principle 3 Task Force on Security by Default.



On top of their countries of establishment, CoT Partners are also active in close to 170 countries worldwide.

The Security by Default Task Force: Our Activities

The principle of "Security by Default" represents one of the ten fundamental principles of the Charter of Trust. The Principle 3 Task Force, consisting of cybersecurity professionals from the Charter of Trust member companies, have come together and worked on several topics related to Security by Default.

The Task Force's work has been split into three phases:

- **Phase 1** focusing on Security by Default for Products, Functionalities and Technologies.
- **Phase 2** focusing on Security by Default for Processes, Operations and Architectures.
- **Phase 3** focusing on Security by Default for Sharing of best practices on Security by Default adoption (Current Phase).

The Task Force has also published documents related to baseline security requirements for phases 1 and 2 and best practices documents in phase 3. The links to the publications can be found below.

Phase 1

- **2020:** Principle 3 - Phase 1 "Products, Functionalities, Technologies" Baseline Requirements.
- **2021:** Achieving Security by Default. An Explanatory Document for the Phase 1 "Products, Functionalities, Technologies" Baseline Requirements.

Phase 2

- **2021:** Achieving Security by Default. An Explanatory Document for the Phase 2 "Processes, Operations, Architectures" Baseline Requirements.
- **2022:** P3 Phase 2 "Processes, Operations, Architectures" Baseline Requirements.

Phase 3

- **2023:** Secure Development Lifecycle: step-by-step guidelines.
- **2024:** Guideline on Cybersecurity Risk Assessment.

Disclaimer

The following document serves as an overview and general information resource only. It is not intended to provide legal advice or guidance of any kind. While efforts have been made to ensure the accuracy and completeness of the information presented herein, it may not encompass all legal nuances or variations applicable to specific circumstances.

Readers are encouraged to consult with qualified legal professionals or advisors regarding their particular situations or concerns. Reliance solely on the information contained in this document is done at the reader's own risk. The author and publisher disclaim any liability for any loss or damage arising directly or indirectly from the use of or reliance on this document.

Objective

In today's intricately connected digital world, cybersecurity is of utmost importance. The threat landscape is constantly evolving, with cyberattacks growing more complex and prevalent. To tackle these challenges, numerous regulations and frameworks are being established and refined globally.

Businesses, especially small and medium ones, often face challenges in keeping up with upcoming regulations and understanding how to address potential security vulnerabilities.

This document, crafted by industry partners at the Charter of Trust, aims to offer a concise overview of current information on significant cybersecurity regulations in various regions worldwide. It focuses on the European Union (EU), Japan, the People's Republic of China (PRC), the Republic of India, the Republic of Singapore, the United Kingdom of Great Britain and Northern Ireland (UK), and the United States of America (USA).

Target audience

The document aims to provide guidance to current or future members of the Charter of Trust and other stakeholders who would like to gain greater insights into the major cybersecurity regulations as part of their Security by Default Strategy.

Overview of Regulations

The following table provides an overview of the regulations in scope of this paper.

REGULATION	IMPORTANT DATES	PAGE
European Union		13
AI Act (AIA)	Entry into force **August 2024**; Forbidden AI by **February 2025**; GPAI obligations **August 2025**; AIS obligations by **August 2026**; all other obligations by **August 2027**	13
Cyber Resilience Act (CRA)	Entry into force **November 2024**; vulnerability reporting by **September 2026**; all other obligations by **December 2027**	13
Cyber Security Act (CSA)	Entry into force & mostly applicable **June 2019**; remain obligations by **June 2021**	14
Data Act (DA)	Entry into force **January 2024**; applicable by **September 2025**	14
Digital Operational Resilience Act (DORA)	Entry into force **January 2023**; applicable by **January 2025**	14
European Cybersecurity Certification Scheme (EUCC, EUCS, EU5G)	Varying	15
Network and Information Systems Security Directive 2 (NIS2)	Entry into force **January 2023**; national transposition until **October 2024**	15
Radio Equipment Directive Delegated Act (RED-DA)	Applicable from **1 August 2025**	16
Vertical Cybersecurity Legislation:		16
Civil Aviation Regulation (EU) 2018/1139	Entry into force **July 2018**; fully applicable since **September 2023**	16
Machinery Regulation 2023/1230 (MR)	Entry into force **July 2023**; applicable by **January 2027**	16
Medical Device Regulation (MDR)2017/745	Since **May 2021** fully applicable except some legacy transitions (2024-2028)	16
India		17
National Cyber Security Policy, 2013	Issued in **2013**	17
The Information Technology (IT) Act, 2000	**2000**	17
The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Rules, 2021”)	**2021**	17
Digital Personal Data Protection Act (DPDP)	**Under Process**	17

CERT-In Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet	Issued in April, **2022**	18
CERT-In Guidelines and relevant Documents	Varying	18
The Telecommunications Act, 2023 and Rules Notified Department of Telecommunications	**2023**	18
Telecommunications (Telecom Cyber Security) Rules, 2024	**2024**	18
Central Electricity Authority (CEA) (Cyber Security in Power Sector) Guidelines, 2021	Issued in **2021**	18
Reserve Bank of India (RBI): Cyber Security Framework for Banks by Reserve Bank of India	Issued in June, **2016**	19
Reserve Bank of India (RBI): Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach	Issued in December, **2019**	19
Reserve Bank of India (RBI): Master Direction on Digital Payment Security Controls	Issued in February, **2021**	19
Reserve Bank of India (RBI): Master Direction on Outsourcing of Information Technology Services	Issued in April, **2023**	19
Reserve Bank of India (RBI): Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices	Issued in November, **2023**	19
Reserve Bank of India (RBI): Cyber Security Controls for Third-Party ATM Switch Application Service Providers	Issued in December, **2019**	19
Securities and Exchange Board of India (SEBI) Cyber Security and Resilience Framework	Issued in August, **2024**	20
Insurance Regulatory and Development Authority (IRDAI) Information and Cyber Security Guidelines, 2023	Issued in April, **2023**	20

Japan		**21**
Basic Act on Cybersecurity	Passed and enacted by the House of Representatives on **November 6, 2014**. The law was fully enforced on **January 9, 2015**.	21
Cybersecurity Policy for Critical Infrastructure Protection (CIP)	The act was published on **June 17, 2022**, and revised on **March 8, 2024**.	21
Economic Security Promotion Act	The act was published on **May 18, 2022**. Implementation of the act was **within 6 months to 2 years from the publication date**.	21
People's Republic of China		**22**
Critical Network Devices Security Common Requirements	Publishing Date **February 20, 2021** Effective Date **August 1**, **2021**	22
Cryptography Law	Publishing Date **October 26**, **2019** Effective Date **January 1**, **2020**	22
Cybersecurity Law	Publishing Date **November 7**, **2016** Effective Date **June 1**, **2017**	22
Cybersecurity Review Measures	Publishing Date **November 16**, **2021** Effective Date **February 15, 2022**	22
Data Security Law	Publishing Date **June 10, 2021** Effective Date **September 1, 2021**	22
Measures for Security Assessment of Data Cross-border Transfer	Publishing Date **July 7, 2022** Effective Date **September 1**, **2022**	22
Personal Information Protection Law	Publishing Date **August 20**, **2021** Effective Date **November 1**, **2021**	22
Provisions on Facilitating and Regulating Cross-border Data Flows	Publishing Date **March 22**, **2024** Effective Date **March 22**, **2024**	20
Regulation of Security Protection of Critical Information Infrastructure	Publishing Date **July 30, 2021** Effective Date **September 1**, **2021**	22
Security Technical Requirements for Specialized Cybersecurity Products GB 42250-2022	Publishing Date **December 29, 2022** Effective Date **July 1, 2023**	22

Singapore		**23**
Computer Misuse Act (CMA)	Enacted in **1993**, amended twice between **1994** and **2012.**	23
Cybersecurity Act	**2018**, amended in **May 2024**.	23
Personal Data Protection Act (PDPA)	Enacted initially in **2012** and later amended in **2020**, the law was implemented in phases. The first phase of amendments took effect on **February 1, 2021**.	23
United Kingdom		**24**
Product Security and Telecommunications Infrastructure Act (PSTI)	Since **April 2024** fully applicable	24
United States		**25**
DHS CISA Guidance	Published **2023**	25
Executive Order EO 14028	Issued on **May 12, 2021**.	25
NIST Cybersecurity Framework (CSF)	Initially published in **2014**, Version 1.1, released in **2018**, Version 2.0 published in **2024**.	25
OMB Memorandum	Issued **September 14, 2022.**	26
US Cyber Trust Mark Program	In development	26
International		**26**
UNECE R155 and R156	Published **March 2021**; entry into force **July 2022**; fully applicable since **July 2024.**	26

1. Security by Default as Basis for Regulatory Compliance

“Security by Default” is a principle that emphasizes that security features are designed, implemented and consistently active and functioning throughout the entire lifecycle of a product, service, process, or business model.

The primary goal of major cybersecurity regulations is to establish robust security measures that safeguard individuals, infrastructure, and organizations, while also protecting sensitive data. By having security measures enabled by default, organizations can demonstrate a proactive and consistent commitment to protecting sensitive data and maintaining compliance with relevant laws and standards.

Our CoT Security by Default Task Force has consistently advocated for this approach through various publications, including baseline security requirements for products, processes, and organizations, as well as guidance documents to facilitate their implementation.

Our Task Force has also shared best practices from industry members on topics such as cyber risk assessment and secure software development lifecycle. These subjects form the cornerstone of numerous regulations currently in development. Consequently, "Security by Default" not only serves as a foundation for regulatory compliance but is also an essential requirement for adhering to certain regulations and ensuring adequate security measures at all levels.

2. Cybersecurity Regulations

The increased usage of IT devices, services, and processing in our daily lives is having a significant impact on the economy, infrastructure, and society. The integration of technology in every facet of our lives, from healthcare to transportation, carries with it inherent risks. As our dependence on technology grows, potential cybersecurity threats on human safety and health are increasing as well. The need to mitigate these risks is a key driver for the introduction of new cybersecurity legislation. Additionally, the rise in the number of cyberattacks, whether for financial gain, such as those carried out by cybercriminals, or for activism purposes, known as 'hacktivism,' is another primary motivator. Particularly concerning are the increasingly powerful attacks happening on a geopolitical level, often referred to as cyberwarfare. These attacks can have severe consequences, and their increasing frequency and power necessitate robust cybersecurity legislation.

Cybersecurity regulations are being imposed by states for several reasons. For one, cybersecurity is often not understood by customers and consumers and therefore not valued or requested. This lack of demand means that many IT manufacturers do not prioritize cybersecurity measures in their products. Additionally, the owners of cybersecurity costs are not always those impacted by cyberattacks, creating a potential competitive advantage for those that choose to ignore cybersecurity measures. The technical and legal landscape is also inconsistent, and cybersecurity remains a relatively new and evolving field of research for many use cases (e.g., product cybersecurity).

The fundamental aim of introducing basic cybersecurity regulations is threefold. Firstly, regulations aim to ensure a common baseline cybersecurity protection for all IT devices and services, providing a minimum standard of security that must be met. Secondly, regulations aim to increase the resilience of the economy, supply chains, infrastructures, and society against cyberattacks. By enforcing minimum cybersecurity standards, the potential impact of cyberattacks can be mitigated, and the overall resilience of these areas improved. Lastly, regulations aim to ensure fair competition by including a common minimum protection level and a common cybersecurity conformity evaluation.

By harmonizing the technical and legal cybersecurity landscape, all players must meet the same basic requirements, creating a fairer and more secure digital environment.

As most countries and relevant organizations recognize the critical importance of cybersecurity, they are enacting regulations to address these challenges. However, approaches vary significantly across regions, reflecting different priorities and legal frameworks. In the following, it will be explored how different regions and countries are handling the development of cybersecurity legislation and their efforts to mitigate cyber risks.

2.1 European Union

In recent years, the European Union (EU) is developing numerous IT-related regulations and directives due to the increasing frequency and severity of cyberattacks on a growing number of connected devices. These attacks have a “critical impact not only on the Union’s economy, but also on democracy, consumer safety and health.”[2]

In the following, a selection of important European cybersecurity regulations and directives can be found.

Artificial Intelligence Act (AIA)

The European AI Act, officially published in the EU Official Journal on July 12, 2024, came into force on August 1, 2024. This triggered the implementation deadlines for the Act's requirements. The first deadline, February 1, 2025, mandates the prohibition of certain "prohibited" AI applications, making their use illegal within the EU after this date. This reinforces the EU's commitment to regulating AI based on risk, prioritizing safety and ethical considerations.

The phased approach allows stakeholders time to adapt, with subsequent deadlines for General Purpose AI and high-risk AI systems still approaching. This initial ban underscores the urgency of addressing potential AI harm. The remaining timelines pressure businesses to assess their AI usage, classify systems, and implement necessary changes for compliance and trustworthy AI.

The AI Taskforce of the Charter of Trust is one of these initiatives that are actively working to support companies in their AI journey. As a cross-industry initiative focused on building trust in digital technologies, the CoT plays a crucial role in providing guidance and best practices for implementing the AI Act. Their expertise contributes to a smoother and more effective implementation process for organizations navigating the complexities of the new regulation.

Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) is one of the worldwide first legislations that enforces cybersecurity for all digitally connected products made available at the EU market. The CRA applies to all digital hardware and software products that are placed on the EU market including consumer products like smartphones and home appliances, but also to industrial control systems, or operating systems that not yet fall under any sector-specific cybersecurity regulation (e.g., vehicles already in scope of UNR155 or medical devices already in scope of MDR).

The CRA uses a harmonized legal framework (called “NLF”) that enforces a set of technical cybersecurity requirements and two obligatory cybersecurity processes – one for ensuring a secure product lifecycle including secure design, development, production, and operation, and another for ensuring vulnerability management including vulnerability monitoring, vulnerability reporting, and free security updates for at least five years or the support period of the product (except for tailor-made products).

Depending on the cybersecurity risk in case of a successful cyberattack, the EU has defined four different paths to demonstrate compliance with the CRA. Most of the products will fall under the ‘default category’ and can prove conformity using a self-declaration. Product categories which are considered more critical might need a third-party evaluation or even certification according to EU CSA based EU Cybersecurity Certification Schemes enacted under the EU CRA.

The CRA will become applicable already in September 2026 regarding the vulnerability reporting obligations and in December 2027 for all other cybersecurity requirements and obligations.

[2] Cf. European Cyber Resilience Act (CRA), Position of the European Parliament adopted at first reading on 12 March 2024, Recital (1).

Cyber Security Act (CSA)

The Cyber Security Act (CSA) has been issued in 2019 to establish the European cybersecurity agency ENISA (European Union Agency for Cybersecurity) that acts as central public authority regarding cybersecurity in Europe (including oversight on national CSIRTs), and to provide a common, legal framework for official cybersecurity certifications of IT services and IT products at the EU (cf. EUCC).

Data Act (DA)

The EU Data Act, a key component of the European data strategy, came into force on January 11, 2024. It advances the Digital Decade's digital transformation goals and complements the Data Governance Act, which facilitates voluntary data sharing. Together, these acts ensure reliable and secure data access, fostering its use in key economic sectors and public interest areas, contributing to an EU single market for data.

The Data Act's provisions will become applicable on September 12, 2025, following a 20-month transition period to give businesses time to meet its requirements. By mandating that connected products be designed in a way that allows users to easily and securely access, use, and share data, it establishes fair rules for data access and use that are crucial with the rise of IoT. This cross-sectoral legislation sets universal principles that should guide future regulations.

The Data Act is structured into nine main chapters following the general provisions that set out its scope and define key terms:

- Chapter I: General Provisions: Defines the scope and key terms of the Act.
- Chapter II: Business-to-Business and Business-to-Consumer Data Sharing in IoT: Users of IoT devices can access, use, and port data generated through their use of connected products.
- Chapter III: Business-to-Business Data Sharing: Clarifies data-sharing conditions when businesses are legally obliged to share data with other businesses.
- Chapter IV: Unfair Contractual Terms: Protects businesses, particularly SMEs, from unfair contractual terms imposed on them.
- Chapter V: Business-to-Government Data Sharing: Allows public sector bodies to access private sector data in situations of exceptional need, enabling evidence-based decisions.
- Chapter VI: Switching Between Data Processing Services: Requires cloud and edge computing service providers to meet minimum requirements for interoperability and enable easy switching.
- Chapter VII: Unlawful Third Country Government Access to Data: Protects non-personal data stored in the EU from unlawful access requests by foreign governments.
- Chapter VIII: Interoperability: Ensures data can flow within and between data spaces and establishes an EU repository for relevant standards and specifications for cloud interoperability.
- Chapter IX: Enforcement: Member States must appoint competent authorities to monitor and enforce the Data Act, granting them the power to impose penalties for non-compliance. Each Member state must also designate a 'data coordinator' acting as the single point of contact at the national level.

Digital Operational Resilience Act (DORA)

DORA is an EU regulation that entered into force on January 16, 2023. It creates a binding and comprehensive Information and Communication Technology (ICT) risk management framework for the EU's financial sector. The Act establishes technical standards that Financial Entities (FEs) and their critical third-party technology service providers must implement in their ICT systems by January 17, 2025.

Overall, it applies to financial organizations operating in the EU under 21 categories, amongst which: credit institutions, payment institutions, electronic money institutions, investment firms, insurance and reinsurance undertakings, and others. Notably, DORA also applies to some entities typically excluded from financial regulations such as third-party service providers that supply financial firms with ICT services.

While the EU has officially adopted the regulation, most of the Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) are still under review. Once DORA comes into scope, competent authorities can request that FEs take specific security measures and remediate vulnerabilities. They can impose penalties on entities that fail to comply with it. Each member state will decide on its own penalties. Like competent authorities, lead overseers can request security measures and remediation and penalize non-compliant critical ICT providers.

➔ For further information, please see Appendix A.

European Cybersecurity Certification Schemes (EUCC, EUCS, EU5G)

European cybersecurity certification schemes are used to demonstrate at a high, very formal level that IT products, services and processes adhere to specific cybersecurity-related requirements. Formal cybersecurity certifications are sometimes required to use products and services in (public) high-security areas (cf. “critical products” acc. Art. 8 CRA).

Based on the international Common Criteria framework[3] and introduced by the CSA (cf. above), the EU develops different certification schemes for specific product classes or services. The most prominent ones are the scheme for ICT products (EUCC) based on the Common Criteria, for cloud security (EUCS), and 5G cellular technologies (EU5G).

Network and Information Systems Security Directive 2 (NIS2)

The Network and Information Systems Security Directive 2 (NIS2) is an EU Directive (EU 2022/2555) that aims to improve the overall level of cybersecurity in the EU by setting out a common set of rules for ensuring the security of network and information systems. The NIS2 Directive, which updates the original NIS Directive on Cybersecurity, was adopted by the European Union in December 2022. EU member states were required to transpose the NIS2 Directive into national law by October 17, 2024. Following this, organizations that fall under the directive must have it fully implemented within 6 months, meaning they should be compliant by April 17, 2025. Certain countries provide a transition period, typically lasting 36 months until October 2027, during which businesses must demonstrate their compliance with the new regulations.

The Directive’s primary goals are to enhance cybersecurity of network and information systems across the EU, improve incident response and crisis management capabilities of Member States, increase cooperation and information sharing between Member States, and establish a culture of cybersecurity risk management among organizations.

The Directive sets out several cybersecurity requirements for organizations, including:

1. Risk management
2. Incident response
3. Supply chain security
4. Cybersecurity governance
5. Security measures
6. Vulnerability disclosure
7. Cybersecurity awareness and training.

[3] Cf. https://www.commoncriteriaportal.org.

Organizations must ensure that appropriate technical, operational, and organizational measures are taken for their essential and important entities to protect their network and information systems from unauthorized access, use, disclosure, modification, or destruction. The required measures should be proportionate to the risks faced by the organization and the sensitivity of the data they process. The measures include network security, information system security, data protection, identity and access management, as well as monitoring and incident response.

Organizations must also comply with notification obligations, conduct risk assessments, implement security measures, cooperate with authorities, and maintain records.

➔ A more detailed overview of this directive is provided as part of the Appendix A.

Radio Equipment Directive Delegated Act (RED DA)

The Radio Equipment Directive 2014/53/14 (RED) establishes a regulatory framework for placing radio equipment on the market. Compliance is demonstrated by meeting the essential requirements therein. The initial essential requirements covered safety, EMC and radio performance, but more recently the European Commission adopted a delegated act (EU 2022/30) activating articles 3.3 d, e & f as essential requirements covering cybersecurity of radio equipment.

These additional essential requirements can be summarized as covering protection of the network (3.3d), protection of privacy of the user (3.3e) and protection from fraud.

These requirements become mandatory on 1st August 2025 and apply to most radio equipment, but there are some exceptions depending on the area of application. Medical equipment as well as automotive, marine and road toll systems are out of scope for 3.3 e & f.

After the publication of the delegated act a Standards Request was published by the commission and CEN/CENELEC accepted and began the task of developing harmonized standards for citation in the Official Journal of the European Community (OJEC) which would give a presumption of conformity for products which are fully compliant. If standards are not cited in the OJEC by the mandate date of 1 August 2025, then manufacturers, importers and distributors or radio products onto the European market must use a Notified Body to assist in the assessment of conformity of those products.

Vertical EU Cybersecurity Legislation

Below is a brief list of some other relevant EU cybersecurity legislation that primarily regulates verticals.

Civil Aviation Regulation (CAR)

The (EU) 2018/1139 that regulates design, production, and operation of aircrafts, aerodromes, and aerodromes equipment includes some high-level cybersecurity obligations (cf. Art. 4 (d)). The regulation promotes the assessment of cybersecurity risks, the voluntary exchange of information and cooperation between cybersecurity experts (cf. Art. 88 para. 1) but does not contain any further details on practical implementation.

Machinery Regulation (MR)

The new Machinery Regulation (MR) – that will apply from January 2027 – sets that industrial machinery products in scope of the corresponding regulation (EU) 2023/1230 must now also consider cybersecurity. A new section 1.1.9 named "Protection against corruption" includes dedicated cybersecurity requirements that prevents cybersecurity threats to compromise the safety of machinery function.

Medical Device Regulation (MDR)

European medical devices regulation (MDR) 2017/745 (cf. Annex I) and in-vitro diagnostic regulation (IVDR) 2017/746 (cf. Annex I) introduce dedicated cybersecurity requirements for all medical and IVDR devices incorporating electronic programmable systems and software across their life cycle. The Medical Device Coordination Group (MDCG) composed of representatives of all Member States endorsed a corresponding “Guidance on cybersecurity for medical devices” document (MDCG 2019-16) supporting medical device manufactures to implement necessary cybersecurity requirements.

2.2 India

Government of India has taken several legal, technical, and administrative policy measures for addressing Cyber Security challenges in the country. This includes National Cyber Security Policy (2013), enactment of Information Technology (IT) Act, 2000 and setting-up of Indian Computer Emergency Response Team (CERT-In) as national agency for 24×7 cyber incident responses and cybersecurity functions for the entire Indian cyber community.

Following are the cyber security related regulations, directions & guidelines in India:

Ministry of Electronics and Information Technology (MeitY)

National Cyber Security Policy 2013

The policy sets a comprehensive national approach to cybersecurity, emphasizing protection of critical infrastructure, building capacity, raising awareness, and fostering international and public-private collaboration. The policy is designed to address the growing cyber threats while creating an environment conducive to the development of a secure and resilient digital economy in India.

The Information Technology (IT) Act 2000

The Information Technology Act, 2000 was enacted on 17th Oct, 2000 with a view to provide legal recognition of electronic records, facilitate e-governance, e-transaction and e-commerce and deter computer based crimes. The IT Act has provisions relating to protection of sensitive personal data, exemption from liability to intermediaries, protection of critical information infrastructure, penal provisions for new forms of cybercrime such as obscenity, sexually explicit materials, identity theft, cheating by personation, cyber terrorism, etc. The IT Act has cybersecurity provisions and stringent penalties for cybercrimes such as hacking and identity theft.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021")

The IT Rules, 2021 requires an intermediary to make reasonable efforts by itself and to cause its users to not host, display, upload, transmit, store or share, etc. any information that contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource. The IT Rules, 2021 also require an intermediary to take all measures to secure its computer resource and not knowingly deploy a configuration which may change the normal course of operation. The IT Rules, 2021 also require an intermediary to report any cyber security incident and share related information with the Indian Computer Emergency Response Team (CERT-In) in accordance with the policies & procedures as prescribed and also provide information under its control or possession, or assistance to the Government agency which is lawfully authorized for cyber security activities within the prescribed timelines.

The Digital Personal Data Protection (DPDP) Act, 2023

The DPDP Act, 2023 has been enacted to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. The Act sets forth specific obligations for organizations, especially, regarding the implementation of reasonable security measures to prevent instances of personal data breaches. The DPDP Act emphasizes the necessity of safeguarding of digital personal data in response to increasing digitization and the growing threats of cyber breaches.

Indian Computer Emergency Response Team (CERT-In)

CERT-In under the Ministry of Electronics and Information Technology, serves as the national agency for cybersecurity under the Information Technology Act, 2000. It performs various functions, including the collection and dissemination of cyber incident information, issuing cybersecurity alerts, and coordinating responses to cyber incidents.

CERT-In Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet: The directions include reporting cyber incidents within 6 hours, synchronizing ICT system clocks with Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) and maintaining logs securely for 180 days. It also mandates that Data centers, VPS providers, cloud service providers, and VPN providers must register accurate information and retain it for at least 5 years or as required by law after registration cancellation. Virtual asset service providers, exchange providers, and custodian wallet providers must retain KYC information and financial transaction records for five years.

National Cyber Coordination Centre (NCCC) has been set up in CERT-In to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

CERT-In has launched various initiatives and issued guidelines, some of the recent guidelines are as follows:

- Guidelines for Secure Application Design, Development, Implementation & Operations
- Technical Guidelines on Software Bill of Materials (SBOM)
- Cyber Security Audit Baseline Requirements
- Guidelines for Cyber Security Auditing.
- Cyber security Control Matrix for Procurement of Services & Solutions by Government Organization
- Guidelines on Information Security Practices for Government Entities

Detailed overview of these documents and initiatives is provided as part of the Appendix B.

National Critical Information Infrastructure Protection Centre (NCIIPC)

National Critical Information Infrastructure Protection Centre (NCIIPC) was set up in exercise of the power given under the Information Technology Act, 2000 for protection of critical information infrastructure in the country.

Department of Telecommunications (DOT)

The Telecommunications Act, 2023 and Rules Notified by DOT

The Act to amend and consolidate the law relating to development, expansion and operation of telecommunication services and telecommunication networks; assignment of spectrum; and for matters connected therewith or incidental thereto.

Telecommunications (Telecom Cyber Security) Rules, 2024

Telecom Cyber Security Rules, 2024 aim to establish a comprehensive framework for securing telecommunications networks and systems against cyber threats. These rules outline obligations for telecom service providers, including the creation of cybersecurity policies, regular risk assessments, data protection measures, and the reporting of incidents. They also emphasize stricter security requirements for telecommunications infrastructure, with provisions for regular cybersecurity audits and cooperation with national security agencies.

Central Electricity Authority

Central Electricity Authority (CEA) (Cyber Security in Power Sector) Guidelines, 2021

The Guidelines aim to enhance cyber resilience in India's power sector. They outline strategies to identify, assess, and mitigate cyber risks, emphasizing robust cybersecurity measures to protect critical infrastructure. The guidelines require security controls, incident response mechanisms, and continuous monitoring. They also advise regular cybersecurity audits by CERT-In empaneled auditing organisations to identify gaps and improve security practices.

Reserve Bank of India

Cyber Security Framework for Banks by Reserve Bank of India

The Reserve Bank of India (RBI) has issued below comprehensive cybersecurity frameworks to strengthen the security posture of banks and cooperative banks, focusing on proactive risk management, incident response, and continuous monitoring.

- Cyber Security Framework for Banks: This framework mandates banks to implement a robust cybersecurity policy, approved by the Board, that covers various critical areas such as vulnerability assessments, network security, data protection, and patch management. It emphasizes continuous surveillance, real-time threat defense, and the establishment of a Cyber Crisis Management Plan (CCMP) for incident detection and response. Other key areas include user access management, vendor risk management, and setting up a Security Operations Center (SOC) for effective incident handling.

- Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach: The framework for UCBs classifies institutions into four levels based on their digital depth. with higher levels requiring stricter security controls. Level I UCBs (the smallest) must implement security measures in addition to those prescribed in the 2018 circular, such as email security with DMARC, multi-factor authentication, security review of endpoints, a robust password management policy, employee education, and incident reporting. Level II UCBs are required to implement additional controls, including a data loss prevention strategy, anti-phishing measures, and vulnerability assessment and penetration testing (VA/PT) of critical systems. Level III UCBs must implement advanced real-time threat defense and management, as well as risk-based transaction monitoring. Level IV UCBs, which have the highest digital exposure, are mandated to establish a Cyber Security Operations Center (C-SOC), participate in cyber drills, adopt adequate incident response and management protocols, and implement an IT and IS governance framework with appropriate IT committees, strategies, and policies.

Master Directions by Reserve Bank of India (RBI)

The Reserve Bank of India (RBI) has issued several Master Directions to address various aspects of digital and IT services in the financial sector, ensuring enhanced security, risk management, and regulatory compliance. These include:

- Master Direction on Digital Payment Security Controls
- Master Direction on Outsourcing of Information Technology Services
- Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices

These directions aim to provide a structured approach for regulated entities to manage and safeguard their digital and IT operations effectively.

Cyber Security Controls for Third-Party ATM Switch Application Service Providers

In 2019, the Reserve Bank of India (RBI) mandated that regulated entities ensure their third-party ATM Switch Application Service Providers (ASPs) implement strong cybersecurity controls. These controls address areas like preventing unauthorized software access, network and environmental security, secure configurations, Application Security Life Cycle (ASLC), patch and vulnerability management, data leak prevention, audit logging, incident response, real-time threat defense, C-SOC surveillance, forensic readiness, and compliance with standards like PCI-DSS and PA-DSS where applicable.

Detailed overview of these documents and initiatives is provided as part of the Appendix B.

Securities and Exchange Board of India (SEBI)

Securities and Exchange Board of India (SEBI) Cyber Security and Resilience Framework

SEBI's Cyber Security and Resilience Framework aims to protect data integrity, market stability, and investor confidence. It requires securities market institutions to implement strong cybersecurity measures, including risk assessment, incident response, and regular audits. The framework promotes the adoption of international best practices, continuous monitoring, and capacity building to address emerging risks, ensuring a secure and resilient securities market.

Insurance Regulatory and Development Authority (IRDAI)

Insurance Regulatory and Development Authority (IRDAI) Information and Cyber Security Guidelines, 2023

The IRDAI Information & Cyber Security Guidelines, 2023 aim to strengthen the insurance sector's defenses against cyber threats through a risk-based approach. These guidelines, applicable to insurers, intermediaries, and other regulated entities, focus on governance, cyber risk management, and data protection. They mandate controls on data classification, storage, access, and handling, as well as the creation of a cyber-crisis management plan for incident response. The guidelines emphasize a "Security by Design" approach, ensuring that security is integrated into systems from the start, with measures like encryption, access control, and regular updates to address vulnerabilities. Additionally, third-party service providers must align with security policies, and annual audits ensure ongoing compliance.

Detailed overview of these documents and initiatives is provided as part of the Appendix B.

2.3 Japan

In Japan, similar to the U.S., the focus has been on encouraging the private sector to adopt cybersecurity measures through guidelines rather than strict regulations. However, due to increasing cyber-attacks on factories and critical infrastructure, the government has introduced mandatory cybersecurity regulations for specific sectors, such as electric power and gas facilities, starting from 2016. National laws have also been amended to incorporate cybersecurity requirements for the automotive and shipbuilding industries. To enhance economic resilience, the Economic Security Promotion Act was enacted in 2022, which includes measures like prior government review for new critical infrastructure projects and the expected introduction of a security clearance system for accessing sensitive information.

Basic Act on Cybersecurity

The Basic Act on Cybersecurity, enacted in 2014, mandates that the Japanese government develops and implements a comprehensive cybersecurity strategy, with critical infrastructure providers required to adopt cybersecurity measures. This law establishes foundational principles of cybersecurity policy, clarifies the roles and responsibilities of government, private entities, and citizens, and creates a framework for cybersecurity policy, including the formulation of strategies and the establishment of the Cybersecurity Strategic Headquarters.

Cybersecurity Policy for Critical Infrastructure Protection (CIP)

Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) has developed a comprehensive policy aimed at protecting the country's critical infrastructure from cyber threats. This policy establishes a strategic framework focused on proactive measures, risk management, and collaboration between government entities, private sectors, and international partners. It includes protocols for incident response, mechanisms for sharing cybersecurity information, and the enforcement of regulations tailored to critical infrastructure sectors. The policy also encourages the adoption of advanced technologies and comprehensive risk management practices to strengthen defenses against cyber threats.

Additionally, the NISC policy emphasizes the importance of continuous evaluation and improvement of cybersecurity measures to adapt to the evolving threat landscape. It underscores the need for regular training and development programs to enhance the skills of personnel responsible for critical infrastructure protection. By advocating for a collaborative approach and emphasizing the critical role of cybersecurity in national security and public safety, the policy ensures the reliability and safety of essential services, which are vital to Japan's national security and public welfare.

➔ A comprehensive graphical outline of the CIP is provided as part of the Appendix C.

Economic Security Promotion Act

The Economic Security Promotion Act is a comprehensive policy aimed at strengthening the country's economic security by addressing vulnerabilities in supply chains, critical infrastructure, and technological innovation. The act introduces measures to secure critical supply chains, enhance the resilience of infrastructure, and encourage the development and protection of advanced technologies essential for Japan's economic interests. It emphasizes the importance of government-private sector collaboration to effectively implement these measures and includes protocols to strengthen information security and protect sensitive data from cyber threats.

Additionally, the act advocates for robust risk management strategies and establishes a supportive regulatory framework to help various sectors adopt and enhance economic security practices. It provides financial incentives and support to businesses, promotes ongoing risk monitoring, and highlights the need for continuous assessment to stay ahead of emerging threats. The policy also underlines the significance of global cooperation in addressing and mitigating international economic security challenges, making it a crucial step towards enhancing Japan's economic resilience against external threats.

2.4 People's Republic of China

The regulatory framework of China's cybersecurity has been set up with three key laws and one key regulation, the Cybersecurity Law effective on June 1, 2017, the Data Security Law effective on September 1, 2021, the Personal Information Protection Law effective on November 1, 2021, and the Regulation of Security Protection of Critical Information Infrastructure (CII) effective on September 1, 2021. Under the regulatory framework, there are many regulations and standards to implement concrete requirements from the laws and facilitate the implementation of the requirements, e.g.

- The Cryptography Law effective on January 1, 2020
- The Cybersecurity Review Measures effective on June 1, 2020
- The Measures for Security Assessment of Data Cross-border Transfer effective on September 1, 2022
- The Provisions on Facilitating and Regulating Cross-border Data Flows effective on March 22, 2024
- The Critical Network Devices Security Common Requirements GB40050-2021 effective on August 1, 2021
- The Security Technical Requirements for Specialized Cybersecurity Products GB 42250-2022 effective on July 1, 2023, etc.

The regulatory framework of China's cybersecurity covers a broad spectrum of industries, including digital infrastructure, big data, data security, financial services, blockchain technology, etc. It is also constantly evolving to effectively govern the progress of emerging industries. Drawing strength from the legislative pillars, China primarily regulates AI technologies through three key regulations:

1. The Internet Information Service Algorithm Recommendation Administrative Measures effective on March 1, 2022
2. The Internet Information Service Deep Synthesis Administrative Measures for deep synthesis algorithms effective on January 11, 2023, and
3. The Interim Measures for generative AI effective on August 15, 2023.

Under the regulatory framework, several policy documents have been issued, such as "Measures for Network Security Review" and "Measures for Cloud Computing Service Security Assessment", which led to the establishment of several crucial systems to safeguard critical information infrastructure, network security review, cloud computing service security assessment, data security management, and personal information protection. Currently, the regulatory framework encompasses more than 150 laws and regulations, along with over 300 national cybersecurity standards. It is expected to reach 1,000 laws, regulations, and standards in the upcoming years.

The regulatory framework elaborates the obligations, responsibilities, processes, requirements, etc., for the stakeholders (organizational, individual, and societal) as network operators, product & service providers, data handlers, authorities, etc., and the elements (equipment, system, service, resources, technology, etc.) in the cybersecurity field, by major relevant government authorities (CAC, MIIT, MPS, SAMR, etc.) and the National Information Security Standardization Technical Committee (TC260) with more than 110 organizational members from governments, institutes, universities, companies, and so on.

Network product & service providers, network operators, and data handlers in the regulatory framework, shall comply with all regulatory requirements for its business and internal operation, specifically, regulatory compliance for all business portfolios, fulfilling Classified Protection of Cybersecurity, Critical Information Infrastructure (CII) protection, data protection & cross-border transfer (incl. VPN), personal information protection, security incident & vulnerability management, cryptographic and AI relative requirements.

2.5 Singapore

Singapore, as a global digital hub, prioritizes cybersecurity and data protection to support its Smart Nation vision. To tackle cyber threats and safeguard privacy, it has established key regulations: the Computer Misuse Act (CMA), the Cybersecurity Act, and the Personal Data Protection Act (PDPA). These laws ensure a secure and trusted digital environment while fostering innovation and growth.

Computer Misuse Act (CMA)

The Computer Misuse Act (CMA) was enacted in 1993 to criminalize unauthorized access or modification of computer material, and other computer crimes. In 2013, the CMA was amended to include cybersecurity measures and renamed the Computer Misuse and Cybersecurity Act (CMCA).

The CMCA criminalizes offences such as: unauthorized access to computer, accessing a system with the intent to commit or facilitate an offence, unauthorized modification of computer material, interception of a computer service, unauthorized disclosure of computer codes, disclosing the credential of another person.

Cybersecurity Act

The Cybersecurity Act (2018), the basic law, requires critical infrastructure providers to comply with the Cybersecurity Code of Practice (CCoP) security guidelines.

In May 2024, an amendment to the legislation was made to expand the applicability of the CCoP to include entities of special cybersecurity interest and foundational digital infrastructure. The objective of the amendment is to extend the oversight of the government over any computer system that is critical to the nation and at high risk of cyberattacks.

The designation of cybersecurity interest entities will be based on the assessment by the government and may potentially include Data Centers and cloud computing infrastructure.

Personal Data Protection Act (PDPA)

The Personal Data Protection Act (PDPA) is Singapore's law that protects personal data, regulates its use by organizations, and includes a Do Not Call (DNC) Registry, allowing individuals to opt out of receiving unsolicited telemarketing messages. The PDPA covers personal data in both electronic and non-electronic formats. It generally does not apply to any individual acting on a personal/domestic basis, any individual acting in his/her capacity as an employee with an organization, public agency data, and business contact information.

The PDPA mandates that organizations must comply with 11 main data protection obligations when collecting, using, or disclosing personal data. These include the following obligations: Accountability, Notification, Consent, Purpose Limitation, Accuracy, Protection, Retention Limitation, Transfer Limitation, Access and Correction, Data Breach Notification, and Data Portability.

The 2022 amendments to the PDPA have increased financial penalties for data breaches and enhanced the enforcement powers of the PDPC. The financial penalties for breaches have a cap of up to 10% of the organization's annual turnover in Singapore, in any other case, S$1 million, whichever is higher.

➔ A more detailed overview is provided as part of Appendix D.

2.6 United Kingdom

The United Kingdom (UK) has been very active in raising awareness as well as in developing and implementing legislation for cybersecurity of IoT devices and was one of the first countries in the world to provide targeted information to consumers of IoT devices in the form of the Code of Practice for IoT Security. Latter has also been used as a benchmark reference worldwide which ultimately resulted in the PSTI.

Product Security and Telecommunications Infrastructure Act (PSTI)

The UK Product Security and Telecommunications Infrastructure (PSTI) Act became mandatory on April 29, 2024. The legislation comes in 2 parts. Part 1 is the section specifically concerned with Product Security. It requires all manufacturers, importers, and distributors of consumer IoT products to ensure that the products they place on the market in the UK are compliant with the security requirements of the legislation. The security requirements details are outlined in Statutory Instrument 2023 No.1007 on consumer protection. The specific details are abridged as:

- **Security Requirement 1** - Ban universal default passwords and easily guessable default passwords
- **Security Requirement 2** - Mandate that manufacturers make available information on how to report security vulnerabilities
- **Security Requirement 3** - Mandate that manufacturers provide transparency on for how long, at a minimum, the product will receive security updates

These security requirements are derived from ETSI EN 303 645 and ISO 29147 and provide a basic level of security. There is a requirement to provide a Statement of Compliance (SoC) to accompany the product when it is placed on the market. Failure to comply with the overall requirement of the PSTI could potentially result in severe penalties which could be the greater of £10 million or 4% of worldwide revenue.

The scope of the PSTI is “consumer products” but other products which may not be directly considered as a traditional consumer product, as they are not directed at consumers, could possibly be considered in scope if they can reasonably be expected to be used by a consumer.

A set of explanatory notes was prepared by the then Department for Digital, Culture, Media and Sport (DCMS) which serves to provide the reader with assistance in understanding the Act. It further aims to explain what the Act means in practice, but does not form part of the Act itself, and is meant for guidance only.

2.7 United States

The U.S. emphasizes cybersecurity through initiatives like DHS CISA's "Security-By-Default" guidance, Executive Order 14028, and the NIST Cybersecurity Framework (CSF). These efforts focus on secure software, zero-trust architecture, and supply chain security. Programs like the OMB's software standards and FCC's Cyber Trust Mark for IoT devices further promote security by design, ensuring a safer digital ecosystem.

DHS CISA Guidance

While not a regulation, the guidance issued by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA) sparked the effort of the Security-By-Default pledge for software manufacturers to sign in the effort to shift the responsibility of secure software away from consumer. Therefore, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the cybersecurity authorities of Australia (Australian Cyber Security Centre), Canada (Canadian Centre for Cyber Security), United Kingdom (NCSC), Germany (BSI), Netherlands (NCSC), published a document titled "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default" in 2023.

The authoring agencies provide joint guidance to software manufacturers, emphasizing the importance of shipping products that are secure by design and default. The goal is to create a safer future for customers, where technology and associated products are designed with security in mind and only secure-by-design and -default products would be shipped to customers.

Executive Order EO 14028

Executive Order 14028, entitled "Improving the Nation's Cybersecurity," aims to enhance the cybersecurity and software supply chain integrity of the U.S. by implementing several key measures designed to bolster the nation's defenses against cyber threats and improve the overall security posture of critical infrastructure and federal systems. Issued on May 12, 2021, the order mandates the following measures:

- Enhancing incident and threat information sharing between service providers and government,
- Adopting secure cloud services and zero-trust architecture with a mandate to deploy multifactor authentication and encryption,
- Establishing baseline security standards for software sold to the government,
- Creating a Cybersecurity Safety Review Board,
- Developing a standardized cyber incident response playbook,
- Improving detection of malicious activity on federal networks,
- Implementing cybersecurity event logging requirements, and
- Requiring amendments to the Federal Acquisition Regulation to align with requirements in the Executive Order.

NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) is not a mandatory compliance but a voluntary framework for everyone to use and customize to their unique needs. NIST CSF serves as a global benchmark for organizations, even though it was originally intended for use by critical infrastructure sectors like healthcare, utilities, and manufacturers. However, many countries now have recognized this and adopted the framework. It evolved successfully from its initial version of NIST CSF v1.0 (Year 2014), updated to v1.1(Year 2018) and now recently to NIST CSF 2.0 February 2024). The NIST CSF 1.0 started off with simple five key functions: Identify, Protect, Detect, Respond, and Recover.

Now the recently released NIST CSF 2.0 includes the "Govern" function, which emphasizes Cybersecurity Governance, Supply Chain Risk Management, and improved controls implementation. Governance includes assessing the organization's present cybersecurity maturity and plots it towards target maturity level.

The NIST Framework approach is closely aligned with the EU Network and Information Systems (NIS) Directive (implemented in the UK as the NIS Regulations) for operators of essential services (OES) and digital service providers (DSP). Also, the NIS Regulations objectives are supported by the UK National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) document.

OMB Memorandum on Enhancing the Security of the Software Supply Chain

The Office of Management and Budget (OMB) "Memorandum on Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (Issued September 14, 2022) was directed by President Biden's EO 14028 "Improving the Nation's Cybersecurity", which directs Federal agencies to comply with "NIST Guidance", defined as Secure Software Development Framework (SSDF) and NIST Software Supply Chain Security Guidance publications, as well as any subsequent updates to be released by NIST. It also directs agencies to use only software that complies with secure software development standards, creates a self-attestation form for software producers to ensure that agencies only use software provided by producers who attest to complying with NIST guidance.

US Cyber Trust Mark Program

Another relevant item is the Federal Communications Commission's (FCC) U.S. Cyber Trust Mark Program voluntary cybersecurity labeling program for wireless IoT devices. Through this program, the FCC will certify that a qualifying IoT product meets certain cybersecurity standards and grant said product the U.S. Cyber Trust Mark label.

2.8 International industry-specific Regulations

The automotive industry has developed one of the few globally applicable product cybersecurity regulations. Specifically, there are the following two UNECE (United Nations Economic Commission for Europe) regulations that set binding requirements for the cybersecurity of vehicles and vehicle manufacturers for the approval of vehicles in their area of application since 2024.

UNECE R155 and R156

- **UNECE R155:** Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system.
- **UNECE R156:** Uniform Provisions Concerning the Approval of Vehicles with Regards to Software Update and Software Updates Management System.

To implement and verify these legal requirements in practice, the international standard ISO/SAE 21434 "Road vehicles – Cybersecurity engineering"[4] has been developed and established.

[4] Cf. https://www.iso.org/standard/70918.html.

3. Conclusion

In today's digitized world, cybersecurity plays a pivotal role in maintaining global stability, economic resilience, and individual privacy. Various regulations have been implemented to safeguard individuals, businesses, and infrastructure from the ever-evolving cyber threats. Each regulation mentioned in this document, though varying in scope and focus by region, aims to protect against potential breaches, data leaks, and other malicious activities that could disrupt operations and compromise sensitive information.

The principle of Security by Default, as advocated by the Charter of Trust, provides a universal standard for organizations to meet compliance requirements effectively. By embedding security measures from the outset, organizations can ensure compliance with regulations, foster trust with customers, safeguard their operations, and strengthen their market position. This approach not only helps organizations meet their legal obligations but also enhances their reputation and competitive advantage.

However, this publication has shown that regulators worldwide have taken different approaches to pursue common cybersecurity goals, leading to varied and sometimes conflicting regulatory frameworks. This complexity can make it challenging for organizations to navigate the cybersecurity landscape and ensure compliance with all relevant regulations.

Albeit not claiming to be exhaustive, this document serves as a roadmap to better navigate this complex landscape, thereby highlighting the benefits of aligning current cybersecurity regulations worldwide.[5] It supports the Charter of Trust's mission to create a secure digital environment for innovation. By using the guidelines outlined in this document, organizations can effectively manage their cybersecurity risks, protect their assets, and contribute to a more secure digital world.

[5] See also the Charter of Trust publication on Harmonization of Regulation - A Charter of Trust perspective.

4. List of References

International

- Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (UNECE R155): https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
- Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system (UNECE R156): https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

Europe

- Cyber Resilience Act (CRA): https://eur-lex.europa.eu/eli/reg/2024/2847/oj
- Revised Network and Information Security Directive (NIS2): https://eur-lex.europa.eu/eli/dir/2022/2555
- Cybersecurity Act (CSA): https://eur-lex.europa.eu/eli/reg/2019/881/oj
- Digital Operational Resilience Act (DORA): https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- Data Act (DA): https://eur-lex.europa.eu/eli/reg/2023/2854/oj
- Artificial Intelligence Act (AIA): https://eur-lex.europa.eu/eli/reg/2024/1689/oj
- European Common Criteria-based cybersecurity certification scheme (EUCC): https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj
- Radio Equipment Directive Delegated Act on Cybersecurity (RED-DA): https://eur-lex.europa.eu/eli/reg_del/2022/30/oj
- Medical Device Regulation (MDR): https://eur-lex.europa.eu/eli/reg/2017/745/oj
- Machinery Regulation (MR): https://eur-lex.europa.eu/eli/reg/2023/1230/oj
- Civil Aviation Regulation (CAR): https://eur-lex.europa.eu/eli/reg/2018/1139/oj
- UK Product Security and Telecommunications Infrastructure (PSTI) Act https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

India

- Information Technology Act: https://www.meity.gov.in/content/information-technology-act
- CERT-In Directions under sub-section (6) of section 70B of the IT Act: https://cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
- CERT-In Guidelines for Secure Application Design, Development, Implementation & Operations: https://cert-in.org.in/PDF/Application_Security_Guidelines.pdf
- IRDAI Information and Cyber Security Guidelines: https://irdai.gov.in/document-detail?documentId=3314780
- SEBI Cyber Security and Resilience Framework: https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html
- RBI Cyber Security Framework in Banks: https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721
- RBI: Master Direction on Digital Payment Security Controls: https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12032
- RBI: Master Direction on Outsourcing of Information Technology Services: https://m.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486
- RBI: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices: https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12562
- RBI: Cyber Security controls for Third party ATM Switch Application Service Providers: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT13060CC89309DEC4BFB8B7CBC33FAA05FE5.PDF
- RBI: Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach: https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11772
- CEA Cyber Security in Power Sector Guidelines: https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf
- CERT-In Guidelines on Information Security Practices for Government Entities: https://cert-in.org.in/PDF/guidelinesgovtentities.pdf
- Cyber security control Matrix for Procurement of Services & Solutions by Government Organisations: https://gem.gov.in/news/view_news/366
- Empanelment of information security auditing organization: https://cert-in.org.in/PDF/Empanel_org_2022.pdf
- Cyber Security Audit Baseline Requirements: https://cert-in.org.in/PDF/CyberSecurityAuditbaseline.pdf

People’s Republic of China

- Cyber Security Law: http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm
- Data Security Law: http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html
- Personal Information Protection Law: http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html
- Cryptography Law: https://www.oscca.gov.cn/sca/c100236/2019-10/28/content_1057345.shtml

Singapore

- Computer Misuse Act (CMA): https://sso.agc.gov.sg/Act/CMA1993
- Cybersecurity Act: https://sso.agc.gov.sg//Act/CA2018
- Personal Data Protection Act (PDPA): https://sso.agc.gov.sg//Act/PDPA2012

5. List of Abbreviations

AIA	Artificial Intelligence Act (EU)
AI CS	Artificial Intelligence Cyber Security (China)
BAC	Basic Act on Cybersecurity (Japan)
CAC	Cyberspace Administration of China
CAF	Cyber Assessment Framework (UK)
CAR	Civil Aviation Regulation (EU)
CCMP	Cyber Crisis Management Plan (India)
CCoP	Cybersecurity Code of Practice (Singapore)
CEA	Central Electricity Authority (India)
CERT	Computer Emergency Response Team
CoT	Charter of Trust
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency (US)
CMA	Computer Misuse Act (Singapore)
CRA	Cyber Resilience Act (EU)
CSA	Cyber Security Act (EU)
CSF	Cyber Security Framework (US)
CSL	Chinese Security Law
CSIRT	Computer Security Incident Response Team
DA	Data Act (EU)
DCMS	Department, for Digital, Culture, Media and Sport (UK)
DHS	Department of Homeland Security (US)
DNC	Do Not Call (Singapore)
DORA	Digital Operational Resilience Act (EU)
DPDP	Digital Personal Data Protection Act (India)
DPO	Data Protection Officer (Singapore)
DSL	Data Security Law (China)
DSP	Digital Service Providers
ENISA	European Union Agency for Cybersecurity
EO 14028	Executive Order 14028 on Improving the Nation’s Cybersecurity (US)
EU	European Union
EUCC	Cybersecurity Certification Scheme on Common Criteria (EU)
EUCS	European Union Cybersecurity Certification Scheme

EU5G	EU 5G Cybersecurity Certification
FCC	Federal Communications Commission (US)
FBI	Federal Bureau of Investigation (US)
FE	Financial Entities
ICT	Information and Communication Technology
IRDAI	Insurance Regulatory and Development Authority (India)
IT Act	Information Technology Act (India)
IVDR	In-Vitro Diagnostic Regulation (EU)
MDCG	Medical Device Coordination Group (EU)
MDR	Medical Device Regulation (EU)
MeitY	Ministry of Electronics and Information Technology (India)
METI	Ministry of Economy, Trade and Industry (Japan)
MIIT	China's Ministry of Industry and Information Technology (China)
MR	Machinery Regulation (EU)
MPS	Ministry of Public Security (China)
NCIIPC	National Critical Information Infrastructure Protection Centre (India)
NCSC	National Cyber Security Centre (UK)
NIS	Network and Information Systems
NISC	National Center of Incident Readiness and Strategy for Cybersecurity (Japan)
NIST	National Institute of Standards and Technology (US)
NIS2	Network and Information Security Directive 2 (EU)
NLF	New Legislative Framework
NSA	National Security Agency (US)
OES	Operators of Essential Services
OJEC	Official Journal of the European Community
PDPA	Personal Data Protection Act (Singapore)
PDPC	Personal Data Protection Commission (Singapore)
PRC	People's Republic of China
PSTI	Product Security and Telecommunications Infrastructure Act (UK)
RBI	Reserve Bank of India
RED DA	Delegated Act of the Radio Equipment Directive (EU)
RTS	Regulatory Technical Standards (EU)
SAMR	State Administration for Market Regulation (China)
SBOM	Software Bill of Materials (India)
SEBI	Securities and Exchange Board of India
SME	Small and Medium Enterprise

SoC	Statement of Compliance (UK)
SSDF	Secure Software Development Framework (US)
TC260	National Information Security Standardization Technical Committee (China)
UK	United Kingdom of Great Britain and Northern Ireland
UK PSTI	Product Security and Telecommunications Infrastructure Act (UK)
UNECE	United Nations Economic Commission for Europe
USA	United States of America

6. Appendix

6.1 Appendix A: Additional information on Europe

Digital and Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) is an EU regulation that creates a binding, comprehensive Information, and Communication Technology (ICT) risk management framework for the EU financial sector. DORA establishes technical standards that Financial Entities (FEs) and their critical third-party technology service providers must implement in their ICT systems by 17 January 2025.

DORA applies to financial organizations operating in the EU under the 21 categories, amongst which: credit institutions, payment institutions, electronic money institutions, investment firms, insurance and reinsurance undertakings, and others. Notably, DORA also applies to some entities typically excluded from financial regulations such as third-party service providers that supply financial firms with ICT services.

DORA's objectives are as follows:

- Harmonize the ICT risk management regulations that already exist in individual EU member states.
- Address ICT risk management and third-party risk management in the financial services sector.
- Prevent, detect, respond to, and recover from incidents.
- Establish a framework that ensures the operational resilience of financial entities and critical third parties which provide ICT-related services to financial entities.
- Ensure cross-border cooperation and information-sharing among regulatory authorities.

DORA imposes requirements in the following four different areas and encourages information sharing agreements:

1. **ICT risk management and governance**: Financial entities (FEs) are expected to develop comprehensive ICT risk management frameworks based on the various stages of ICT Risk Management: identification, protection and prevention, detection, response and recovery, training and development, and communication. The regulation also makes the entity's management body responsible for ICT Risk Management. FEs must map their ICT systems, identify and classify critical assets and functions, document dependencies between assets, systems, processes, and providers, as well as conduct continuous risk assessments on their ICT systems, document and classify cyberthreats, and document their steps to mitigate identified risks. Dedicated and comprehensive business continuity policies and disaster and recovery plans should be in place, ensuring a prompt recovery accounting for various cyber risk scenarios, such as ICT service failures, natural disasters and cyberattacks.
2. **Incident reporting and management**: Financial entities need to establish a management process and clear rules for monitoring, managing, logging, classifying, and reporting ICT-related incidents (both to regulators and affected clients and partners). Like for NIS 2 (Network and Information Systems Security Directive 2), they will be required to file three different kinds of reports for critical incidents: an initial report notifying authorities, an intermediate report on progress toward resolving the incident, and a final report analyzing the root causes of the incident.
3. **Operational resilience testing**: Financial entities are expected to establish and maintain a comprehensive digital operational resilience testing program. This program should include vulnerability assessments and scans, open-source analyses, physical security reviews, source code reviews (where feasible), scenario-based tests, compatibility testing, and performance testing. FEs considered critical for the financial system will also need to undergo threat-led penetration testing (TLPT) every three years and include their critical ICT providers as well.

4. **Management of ICT third-party risk**: Financial entities shall adopt and regularly review a strategy on ICT third-party risk, including a policy on the use and monitoring of ICT third-party service providers. Contractual relationships with the ICT third-party providers should contain all the necessary monitoring and accessibility details such as a full-service level description, an indication of locations where data is being processed, etc. When outsourcing critical and important functions, financial entities must negotiate specific contractual arrangements regarding exit strategies, audits and performance targets for accessibility, integrity and security, among other things. The competent authorities are empowered to request FEs to suspend or terminate contracts with non-compliant ICT third-party providers. DORA also introduces an oversight framework for ICT third-party service providers designated as critical, based on criteria determined by the European Commission. These criteria will be used by the European Supervisory Authorities (ESAs), alongside information provided by FEs in their registers of information, to determine the providers that will be designated as critical. The designation decision is expected in H2 2025. Once designated as critical, each provider will have one of the ESAs assigned as a lead overseer, with oversight beginning one month after the provider is notified of its designation.

While the EU has officially adopted DORA, most of the regulatory technical standards (RTS) and implementing technical standards (ITS) are still under review. The final draft technical standards have been submitted to the European Commission, which will now start working on their review with the objective to adopt these technical standards in the coming months.

Once DORA comes into scope, competent authorities can request that FEs take specific security measures and remediate vulnerabilities. They will also be able to impose penalties on entities that fail to comply, with each member state determining its own penalties. Like competent authorities, lead overseers can request security measures and remediation and penalize non-compliant critical ICT providers.

Network and Information Systems Security Directive 2 (NIS 2)

NIS 2 (Network and Information Systems Security Directive 2) a European Union (EU) directive (EU) 2022/2555 that aims to improve the overall level of cybersecurity in the EU by setting out a common set of rules for ensuring the security of network and information systems. NIS 2 is an update to the NIS Directive (2016/1148/EU) and was adopted on December 14, 2022. EU member states were required to transpose the NIS2 Directive into national law by October 17, 2024. Following this, organizations that fall under the directive must have it fully implemented within 6 months, meaning they should be compliant by April 17, 2025. Certain countries provide a transition period, typically lasting 36 months until October 2027, during which businesses must demonstrate their compliance with the new regulations.

The primary goals and objectives of NIS 2 are to:

- Enhance the security of network and information systems across the EU.
- Improve the incident response and crisis management capabilities of Member States.
- Increase cooperation and information sharing between Member States.
- Establish a culture of cybersecurity risk management among organizations.

In Article 21, NIS 2 sets out several cybersecurity requirements that organizations need to comply with, including:

- Risk Management: Organizations must implement a risk management approach to identify, assess, and mitigate cybersecurity risks.
- Incident Response: Organizations must have an incident response plan in place to detect, report, and respond to cybersecurity incidents.
- Supply Chain Security: Organizations must ensure that their supply chain is secure and that third-party providers meet the required cybersecurity standards.

- Cybersecurity Governance: Organizations must have a clear governance structure in place to manage cybersecurity risks and ensure accountability.
- Security Measures: Organizations must implement appropriate security measures to protect their network and information systems, including encryption, access controls, and network segmentation.
- Vulnerability Disclosure: Organizations must have a vulnerability disclosure policy in place to handle reports of vulnerabilities in their systems.
- Cybersecurity Awareness and Training: Organizations must provide regular cybersecurity awareness and training to their employees.

NIS 2 requires organizations to ensure that for essential and important entities appropriate and technical, operational, and organizational measures are taken to protect their network and information systems from unauthorized access, use, disclosure, modification, or destruction. These measures should be proportionate to the risks faced by the organization and the sensitivity of the data they process.

The required measures include the following:

- Network Security: Implement firewalls, network segmentation, access control, IDPS, and encryption to protect the network.
- Information System Security: Implement secure configuration and change management, vulnerability management, patch management, and secure coding practices to protect information systems.
- Data Protection: Implement data encryption, data backup and recovery, and data loss prevention to protect sensitive data.
- Identity and Access Management: Implement IAM systems, multi-factor authentication, and role-based access control to manage user identities and access.
- Monitoring and Incident Response: Implement SIEM systems, incident response plans, and continuous monitoring to detect and respond to security incidents.
- These security measures are not exhaustive, and organizations may need to implement additional measures based on their unique risk profile and industry requirements. The goal is to ensure that organizations have a robust security posture to protect their network and information systems from cyber threats.

These organizations must comply with the following obligations:

- Notification of Incidents
- Under the NIS2 Directive, organizations must report certain types of incidents to the national competent authority and the EU's Computer Security Incident Response Team (CSIRT).
- Reporting to the national competent authority: within 24 hours of becoming aware of the incident, providing information such as incident description, affected systems, and measures taken to mitigate the incident.

In addition to reporting to the national competent authority, organizations must also notify the EU's CSIRT of a notified incident that meets certain criteria. This includes incidents that:

- Affect critical infrastructure or services.
- Have a significant impact on the organization's operations.

- Have the potential to cause significant harm to individuals or the public.
- Are likely to spread to other organizations or countries.

Reporting generally to the EU's CSIRT: within 72 hours of becoming aware of the incident, providing information such as incident description, affected organization, type of incident, and measures taken to mitigate the incident.

Reporting obligations may vary depending on the incident's impact, sector, or industry, and organizations may have additional reporting obligations under national law or regulation.

In addition to the notification obligation, organizations must comply with the following:

- Conduct a Risk Assessment: Organizations must conduct a risk assessment to identify and mitigate cybersecurity risks.
- Implement Security Measures: Organizations must implement appropriate security measures to protect their network and information systems.
- Cooperate with Authorities: Organizations must cooperate with authorities in the event of a cybersecurity incident.
- Maintain Records: Organizations must maintain records of their cybersecurity measures and incidents.
- Considerations: Entity Scope for NIS2 Compliance in Organizations

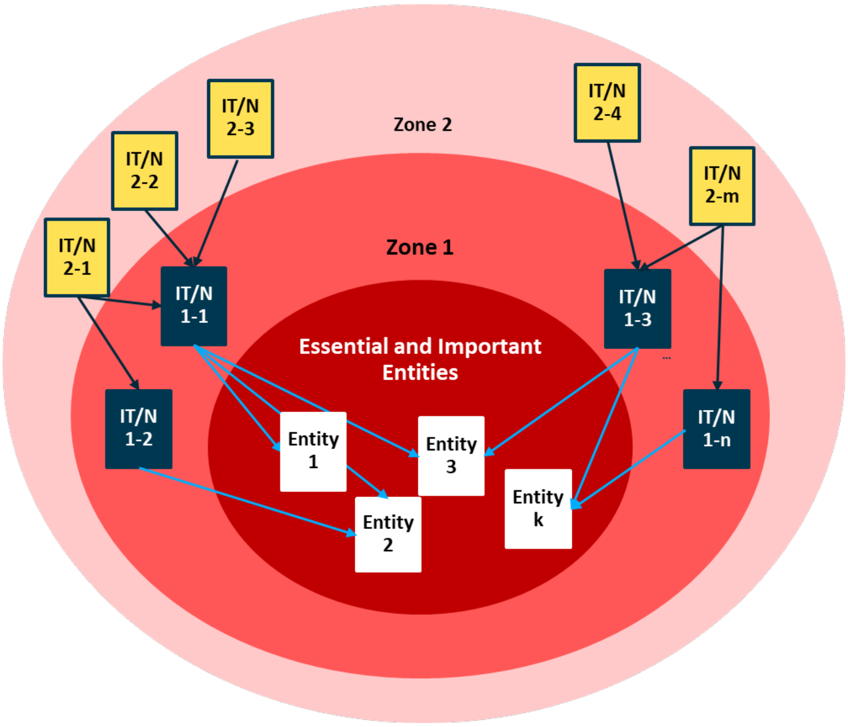
From the regulatory requirements, the scope of the requirements for the organization's IT and network infrastructure can be derived. The scope covers all network and information systems used by essential and important entities of the organization for their operation or for the provision of their services.

These areas can be split into zones (see picture):

Zone 1: IT and network systems that directly support the essential and important entities of the organization in its operation or for the provision of its services fall within the scope of NIS2. For these IT and network systems, the required measures must be taken.

Zone 2: IT and network systems which indirectly support the essential and important entities of the organization in its operation or for the provision of its services, can be within the scope of NIS2. This is to be considered on a case-by-case basis.

Other IT and network systems: These are to be considered on a case-by-case basis according to the risk assessment.



6.2 Appendix B: Additional information on India

Indian Computer Emergency Response Team (CERT-In)

1. **Guidelines for Secure Application Design, Development, Implementation & Operations:** These guidelines aim to establish a strong security baseline throughout the application lifecycle. They require adherence to secure design and development practices before assessments or audits, ensuring proactive security measures are implemented from the start.
2. **Technical Guidelines on Software Bill of Materials (SBOM):** The Guidelines are designed to enhance transparency and security in software supply chains and provide a structured approach for organizations to document and share the components of software, including libraries and dependencies, used in their applications.
3. **Cyber Security Audit Baseline Requirements:** A document outlining minimum security requirements for cyber audits across organizations, categorized by risk levels and security controls.
4. **Empanelment of Auditing Organizations:** CERT-In has empaneled 200 information security auditing organizations for vulnerability assessment and penetration testing of government and critical infrastructure.
5. **Cyber security Control Matrix for Procurement of Services & Solutions by Government Organization** are developed by CERT-In to enable procuring entities to select and include appropriate and applicable controls from the control matrix as per their risk profile and scope of services.
6. **Guidelines on Information Security Practices for Government Entities:** These guidelines provide a roadmap for government entities and industries to reduce cyber risks, protect citizen data, and enhance the cybersecurity ecosystem. They serve as a key resource for auditors to assess an organization's security posture against cybersecurity requirements.

Reserve Bank of India (RBI):

1. **Cyber Security Framework for Banks:** The RBI Cyber Security Framework for Banks mandates banks to establish a comprehensive cybersecurity policy approved by their Board, incorporating strategies to mitigate cyber risks. The framework emphasizes continuous surveillance, vulnerability assessments, and the implementation of a Cyber Crisis Management Plan (CCMP) for incident detection and response. It also prescribes baseline controls for various critical areas, including inventory management of business IT assets, prevention of unauthorized software execution, environmental controls, network management and security, secure configuration, application security life cycle, customer data protection and data leak prevention, patch/vulnerability and change management, user access management, email security, vendor risk management, removable media security, advanced real-time threat defense and management, log management, vulnerability assessment and penetration testing (VA/PT) and red teaming, cybersecurity awareness and anti-phishing measures, setting up of a Security Operations Center (SOC), incident management, and consumer education.
2. **Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach**: The RBI's UCB Graded Approach Cyber Security Framework (2019) builds on the Basic Cyber Security Framework for UCBs issued in 2018. This comprehensive approach classifies UCBs into four levels (I-IV) based on their digital depth, with higher levels requiring stricter security controls. Level I UCBs (the smallest) must implement security measures in addition to those prescribed in the 2018 circular, such as email security with DMARC, multi-factor authentication, security review of endpoints, a robust password management policy, employee education, and incident reporting. Level II UCBs are required to implement additional controls, including a data loss prevention strategy, anti-phishing measures, and vulnerability assessment and penetration testing (VA/PT) of critical systems. Level III UCBs must implement advanced real-time threat defense and management, as well as risk-based transaction monitoring. Level IV UCBs, which have the highest digital exposure, are mandated to establish a Cyber Security Operations Center (C-SOC), participate

in cyber drills, adopt adequate incident response and management protocols, and implement an IT and IS governance framework with appropriate IT committees, strategies, and policies.

3. **Cyber Security Controls for Third-Party ATM Switch Application Service Providers:** Recognizing that many RBI-regulated entities manage their ATM switch ecosystem through third-party ATM Switch Application Service Providers (ASPs), RBI in 2019 mandated that regulated entities ensure their ASPs implement robust cybersecurity controls. The prescribed controls cover various areas such as preventing unauthorized software access, implementing environmental and network security measures, ensuring secure configuration, adopting the Application Security Life Cycle (ASLC), managing patches, vulnerabilities, and changes effectively, implementing a data leak prevention strategy, maintaining comprehensive audit logs, strengthening incident response and management, employing advanced real-time threat defense and management, ensuring continuous surveillance through the establishment of a Cyber Security Operations Center (C-SOC), maintaining forensic readiness, and complying with industry standards such as PCI-DSS and PA-DSS where applicable.

4. **Reserve Bank of India (RBI): Master Direction on Digital Payment Security Controls:** The RBI (Digital Payment Security Controls) Directions, 2021, require regulated entities to establish a robust governance structure for digital payment systems and implement common minimum security standards across various digital payment channels, including internet banking, mobile banking, and card payments. These requirements are technology- and platform-agnostic, ensuring a secure and enabling environment for customers to use digital payment products safely. The framework mandates regulated entities to have a Board-approved policy for digital payment products and services and prescribes controls related to the Application Security Life Cycle (ASLC), authentication framework, fraud risk management, reconciliation mechanisms, customer protection, and specific security measures for internet banking, mobile banking, and card payments.

5. **Reserve Bank of India (RBI): Master Direction on Outsourcing of Information Technology Services:** The RBI Master Direction on Outsourcing of IT Services, issued in April 2023, mandates that banks and financial institutions ensure risk management, data security, regulatory compliance, and accountability when outsourcing IT services, with strict oversight of third-party vendors. The underlying principle is that outsourcing arrangements should not compromise an entity's ability to fulfill its obligations to customers or impede effective supervision by RBI. The framework requires regulated entities to maintain control over outsourced services while ensuring compliance with regulatory requirements. It defines measures related to governance, risk management, evaluation and engagement of service providers, monitoring and control of outsourcing activities, outsourcing agreements, intra-group outsourcing, cross-border outsourcing, and exit strategies. Specific expectations for cloud service adoption include cloud governance, service and technology architecture evaluation, access management, disaster recovery and cyber resilience, security controls, and continuous monitoring. The outsourcing of Security Operations Center (SOC) functions also presents risks, as data may be stored and processed externally by a Managed Security Service Provider (MSSP), reducing visibility for regulated entities. To mitigate these risks, additional controls have been introduced.

6. **Reserve Bank of India (RBI): Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices:** The RBI Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices, issued in November 2023, establishes baseline requirements for IT governance frameworks within regulated entities. It mandates that entities implement a strong IT governance framework aligned with business goals and comprehensive risk management strategies. It also defines the roles and responsibilities of the Board, senior management, head of IT function, and Chief Information Security Officer (CISO). The directive focuses on IT infrastructure and services management, capacity management, project management, data migration controls, cryptographic controls, access controls, teleworking security measures, business continuity and disaster recovery management, IT and information security risk management, vulnerability assessment and penetration testing (VA-PT), cyber incident response and recovery management, and information security (IS) audits.

Insurance Regulatory and Development Authority (IRDAI)

The IRDAI Information and Cyber Security Guidelines, 2023 are issued to strengthen the defenses of the insurance industry against emerging cyber threats through effective governance mechanisms to oversee cyber security efforts of the organisation. These guidelines apply to all insurers, insurance intermediaries, and other regulated entities in the insurance sector. The Guidelines emphasizes on identifying, assessing, and managing cyber risks and comprehensively cover data protection by mandating controls on data classification, storage, and handling to ensure data security. Also, the measures to control access to sensitive information and systems are provided to protect the information assets of the sector.

A detailed procedure for responding to and managing cyber incidents includes having in place a cyber-crisis management plan and reporting of incident within specified timeframe in prescribed format. The key aspect of said guidelines are data centric approach that focuses on securing the data rather than just the network or system it is stored in, Specific guidelines for managing third-party service providers ensures alignment with the organization's security policies and annual independent audits to ensure continuous compliance to guidelines.

The "Security by Design" aspect of the IRDAI Information and Cyber Security Guidelines, 2023 emphasizes that all systems and processes should be designed with security as a fundamental component from the start i.e. security measures should be integrated into the design and architecture of systems. Key aspects of Security by Design include default settings to minimize vulnerabilities, stringent user access controls and data encryption to prevent unauthorized access to sensitive information, regularly updated to address any security vulnerabilities etc. The approach ensures that security is an integral part of the entire lifecycle of systems and processes, reducing the risk of cyber threats.

6.3 Appendix C: Additional information on Japan

The Basic Act on Cybersecurity

The Basic Act on Cybersecurity (2014) is a basic law that requires the government to develop and implement a cybersecurity strategy and for critical infrastructure providers to implement cybersecurity measures. This also sets basic principles of cybersecurity policy, clarifies the responsibilities of the government, private entities and citizens, and stipulates the framework for cybersecurity policy such as the cybersecurity strategy formulation and the establishment of the Cybersecurity Strategic Headquarters.

In Japan, as in the U.S., the focus is on encouraging the private sector through soft law, with various government agencies encouraging organizations to implement cybersecurity measures by providing guidelines rather than laws and regulations. However, in recent years, cyber-attacks on factories and critical infrastructure facilities have become an issue, so the government has initiated regulations (Ministerial Order level) to mandate cybersecurity measures for certain electric power and gas facilities (from 2016).

For the automotive industry, the national laws have been amended in accordance with UN-R 155/156, and type approval (type approval) has started to reflect cybersecurity requirements (2022). For shipbuilding, type approval certification will be initiated by the Classification Society of Japan (ClassNK) based on IACS UR E26/E27 (from July 2024).

In addition, to ensure economic resilience against geopolitical changes, the Economic Security Promotion Act was enacted (in 2022) and will be put into operation gradually (around April to May 2024). In order to ensure supply chain security, new construction of critical infrastructure facilities and outsourcing of their operation now require prior review by the government. In addition, a qualification system based on security clearance is expected to be introduced in the future for access to sensitive security information (currently under deliberation by the Diet as of 2024).

Japan National Center of Incident and Strategy for Cybersecurity (NISC)'s Cybersecurity Policy for Critical Infrastructure Protection (CIP)

Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) has established a comprehensive policy for Critical Infrastructure Protection (CIP) to safeguard against cyber threats. This policy outlines strategic goals, responsibilities, and actions to enhance the security and resilience of Japan's critical infrastructure sectors.

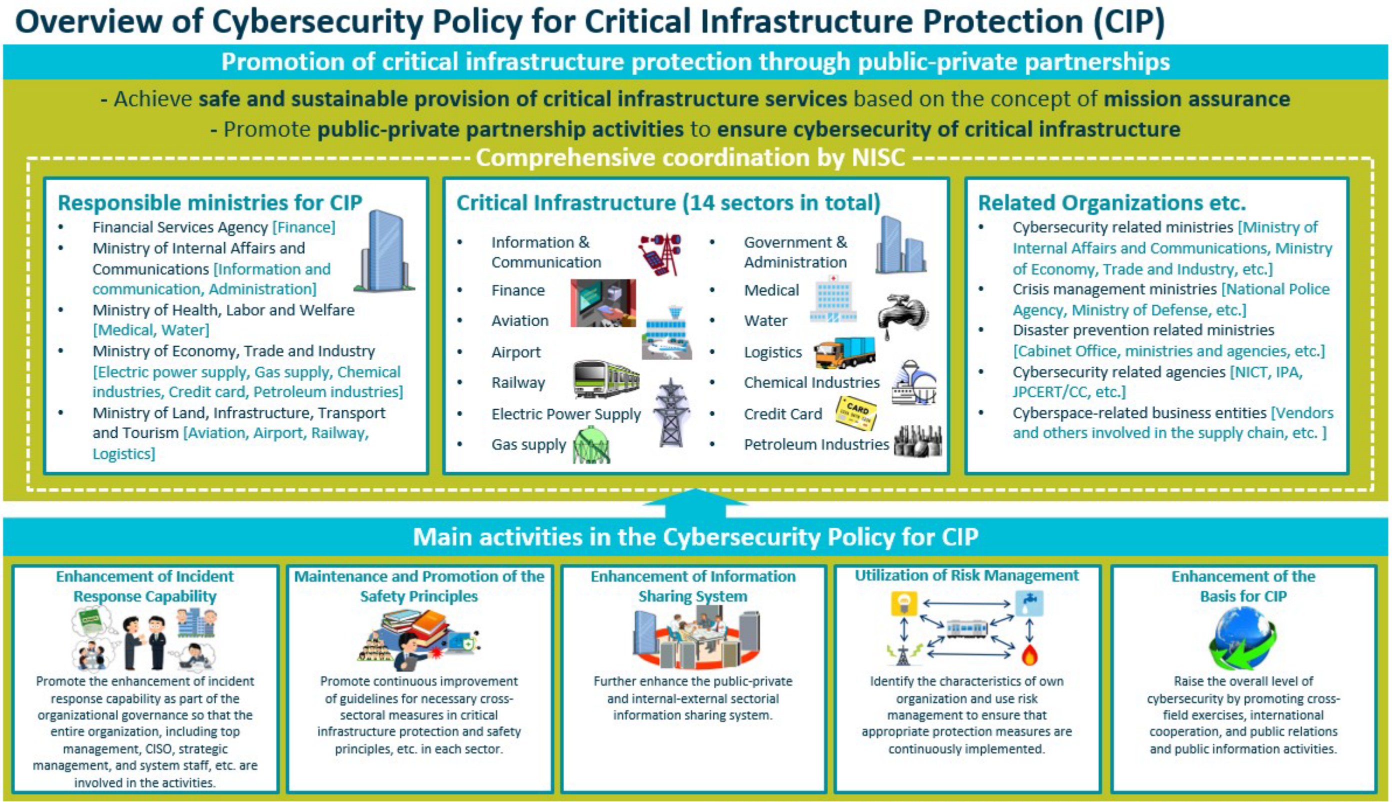
Key Points

- **Strategic Framework:** The policy outlines a strategic framework aimed at enhancing the cybersecurity of Japan's critical infrastructure, focusing on proactive measures and risk management.
- **Government and Private Sector Collaboration:** It emphasizes the need for a collaborative approach between government entities, private sectors, and international partners to effectively tackle cyber threats.
- **Incident Response Protocols:** The policy sets up protocols for immediate and effective response to cybersecurity incidents, ensuring minimal disruption to critical services.
- **Information Sharing Mechanisms:** Promotes robust mechanisms for sharing cybersecurity information and threat intelligence among stakeholders to enhance situational awareness and preparedness.

- **Regulatory Compliance:** Implements and enforces cybersecurity regulations and standards tailored to the needs of critical infrastructure sectors, ensuring compliance and uniformity in security practices.
- **Risk Management Practices:** Encourages the adoption of comprehensive risk management practices to identify, assess, and mitigate potential cyber threats to critical infrastructure.
- **Training and Development:** Provides for regular cybersecurity training and awareness programs to enhance the skills and capabilities of personnel responsible for critical infrastructure protection.
- **Adoption of Advanced Technologies:** Advocates for the integration of advanced technologies and innovative solutions to strengthen cybersecurity defenses and counter emerging threats.
- **Continuous Evaluation:** Calls for ongoing assessment and improvement of cybersecurity measures to ensure they remain effective against the evolving cyber threat landscape.
- **National Security Focus:** Underlines the critical role of cybersecurity in safeguarding national security and public safety, ensuring the continued reliability and trustworthiness of essential services.

Conclusion

The NISC's Cybersecurity Policy for CIP provides a detailed framework aimed at protecting Japan's critical infrastructure from cyber threats. It emphasizes collaboration between government and private sectors, the implementation of robust security measures, and the continuous improvement of cybersecurity practices. The policy is essential for ensuring the reliability and safety of critical services that are vital to national security and public welfare.



Overview of Cybersecurity Policy for Critical Infrastructure Protection (CIP)

Promotion of critical infrastructure protection through public-private partnerships

- Achieve **safe and sustainable provision of critical infrastructure services** based on the concept of **mission assurance**

- Promote **public-private partnership activities** to **ensure cybersecurity of critical infrastructure**

Comprehensive coordination by NISC

Responsible ministries for CIP

- Financial Services Agency [Finance]
- Ministry of Internal Affairs and Communications [Information and communication, Administration]
- Ministry of Health, Labor and Welfare [Medical, Water]
- Ministry of Economy, Trade and Industry [Electric power supply, Gas supply, Chemical industries, Credit card, Petroleum industries]
- Ministry of Land, Infrastructure, Transport and Tourism [Aviation, Airport, Railway, Logistics]

Critical Infrastructure (14 sectors in total)

- Information & Communication
- Finance
- Aviation
- Airport
- Railway
- Electric Power Supply
- Gas supply
- Government & Administration
- Medical
- Water
- Logistics
- Chemical Industries
- Credit Card
- Petroleum Industries

Related Organizations etc.

- Cybersecurity related ministries [Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, etc.]
- Crisis management ministries [National Police Agency, Ministry of Defense, etc.]
- Disaster prevention related ministries [Cabinet Office, ministries and agencies, etc.]
- Cybersecurity related agencies [NICT, IPA, JPCERT/CC, etc.]
- Cyberspace-related business entities [Vendors and others involved in the supply chain, etc.]

Main activities in the Cybersecurity Policy for CIP

Enhancement of Incident Response Capability

Promote the enhancement of incident response capability as part of the organizational governance so that the entire organization, including top management, CISO, strategic management, and system staff, etc. are involved in the activities.

Maintenance and Promotion of the Safety Principles

Promote continuous improvement of guidelines for necessary cross-sectoral measures in critical infrastructure protection and safety principles, etc. in each sector.

Enhancement of Information Sharing System

Further enhance the public-private and internal-external sectorial information sharing system.

Utilization of Risk Management

Identify the characteristics of own organization and use risk management to ensure that appropriate protection measures are continuously implemented.

Enhancement of the Basis for CIP

Raise the overall level of cybersecurity by promoting cross-field exercises, international cooperation, and public relations and public information activities.

Source: National center of Incident readiness and Strategy for Cybersecurity (NISC), 2022

Japan Ministry of Economy, Trade and Industry (METI)'s Economic Security Promotion Act

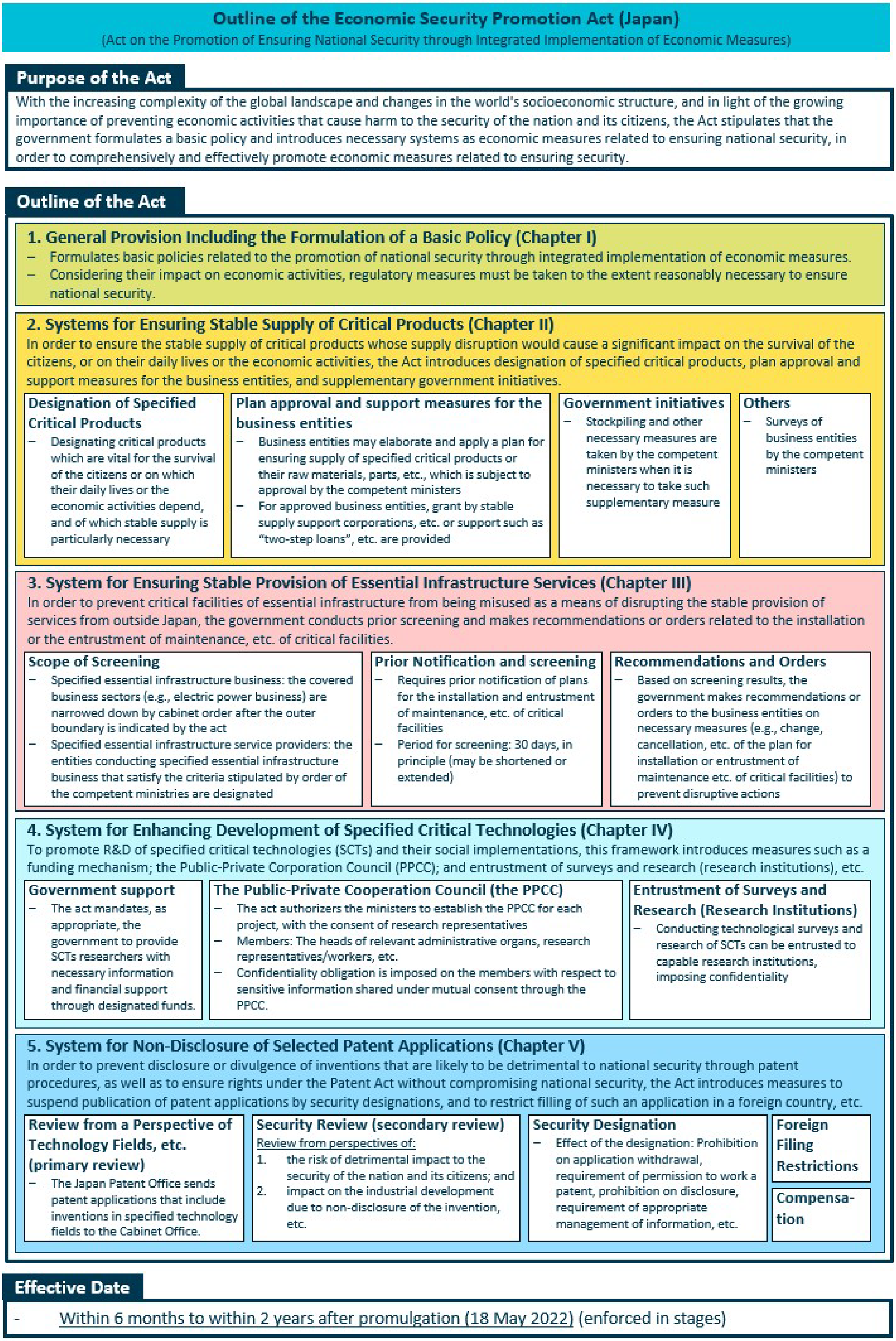
The Economic Security Promotion Act, established by Japan's Ministry of Economy, Trade and Industry (METI), aims to strengthen the country's economic security through various strategic measures. This comprehensive policy addresses vulnerabilities in supply chains, critical infrastructure, and technological innovation to safeguard Japan's economic interests.

Key Points

- **Supply Chain Security Initiatives:** The act introduces measures to secure critical supply chains, ensuring their stability and reliability amidst global uncertainties.
- **Infrastructure Resilience:** Focuses on enhancing the resilience of critical infrastructure against potential threats through comprehensive protection strategies.
- **Technological Advancement:** Encourages the development and safeguarding of advanced technologies essential for maintaining economic security.
- **Government-Private Sector Collaboration:** Stresses the importance of collaboration between the government and private sectors to effectively implement economic security measures.
- **Enhanced Information Security:** Strengthens protocols for information security to protect sensitive data and intellectual property from cyber threats.
- **Risk Management Strategies:** Advocates for the adoption of robust risk management strategies to identify and mitigate economic security risks.
- **Supportive Regulatory Framework:** Establishes a regulatory framework that supports the implementation of economic security measures across various sectors.
- **Financial Incentives and Support:** Provides financial assistance and incentives to businesses to help them adopt and enhance economic security practices.
- **Ongoing Risk Monitoring:** Emphasizes the need for continuous monitoring and assessment of economic security risks to stay ahead of emerging threats.
- **Global Cooperation:** Underlines the importance of international cooperation to effectively address and mitigate global economic security challenges.

Conclusion

The Economic Security Promotion Act is a pivotal legislation designed to enhance Japan's economic resilience against external threats. It includes measures to secure supply chains, protect critical infrastructure, and foster innovation. The act underscores the importance of collaboration between government and private sectors, as well as international cooperation, to effectively safeguard economic security.



Outline of the Economic Security Promotion Act (Japan)

(Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures)

Purpose of the Act

With the increasing complexity of the global landscape and changes in the world's socioeconomic structure, and in light of the growing importance of preventing economic activities that cause harm to the security of the nation and its citizens, the Act stipulates that the government formulates a basic policy and introduces necessary systems as economic measures related to ensuring national security, in order to comprehensively and effectively promote economic measures related to ensuring security.

Outline of the Act

1. General Provision Including the Formulation of a Basic Policy (Chapter I)

- Formulates basic policies related to the promotion of national security through integrated implementation of economic measures.
- Considering their impact on economic activities, regulatory measures must be taken to the extent reasonably necessary to ensure national security.

2. Systems for Ensuring Stable Supply of Critical Products (Chapter II)

In order to ensure the stable supply of critical products whose supply disruption would cause a significant impact on the survival of the citizens, or on their daily lives or the economic activities, the Act introduces designation of specified critical products, plan approval and support measures for the business entities, and supplementary government initiatives.

Designation of Specified Critical Products

- Designating critical products which are vital for the survival of the citizens or on which their daily lives or the economic activities depend, and of which stable supply is particularly necessary

Plan approval and support measures for the business entities

- Business entities may elaborate and apply a plan for ensuring supply of specified critical products or their raw materials, parts, etc., which is subject to approval by the competent ministers
- For approved business entities, grant by stable supply support corporations, etc. or support such as "two-step loans", etc. are provided

Government initiatives

- Stockpiling and other necessary measures are taken by the competent ministers when it is necessary to take such supplementary measure

Others

- Surveys of business entities by the competent ministers

3. System for Ensuring Stable Provision of Essential Infrastructure Services (Chapter III)

In order to prevent critical facilities of essential infrastructure from being misused as a means of disrupting the stable provision of services from outside Japan, the government conducts prior screening and makes recommendations or orders related to the installation or the entrustment of maintenance, etc. of critical facilities.

Scope of Screening

- Specified essential infrastructure business: the covered business sectors (e.g., electric power business) are narrowed down by cabinet order after the outer boundary is indicated by the act
- Specified essential infrastructure service providers: the entities conducting specified essential infrastructure business that satisfy the criteria stipulated by order of the competent ministries are designated

Prior Notification and screening

- Requires prior notification of plans for the installation and entrustment of maintenance, etc. of critical facilities
- Period for screening: 30 days, in principle (may be shortened or extended)

Recommendations and Orders

- Based on screening results, the government makes recommendations or orders to the business entities on necessary measures (e.g., change, cancellation, etc. of the plan for installation or entrustment of maintenance etc. of critical facilities) to prevent disruptive actions

4. System for Enhancing Development of Specified Critical Technologies (Chapter IV)

To promote R&D of specified critical technologies (SCTs) and their social implementations, this framework introduces measures such as a funding mechanism; the Public-Private Corporation Council (PPCC); and entrustment of surveys and research (research institutions), etc.

Government support

- The act mandates, as appropriate, the government to provide SCTs researchers with necessary information and financial support through designated funds.

The Public-Private Cooperation Council (the PPCC)

- The act authorizers the ministers to establish the PPCC for each project, with the consent of research representatives
- Members: The heads of relevant administrative organs, research representatives/workers, etc.
- Confidentiality obligation is imposed on the members with respect to sensitive information shared under mutual consent through the PPCC.

Entrustment of Surveys and Research (Research Institutions)

- Conducting technological surveys and research of SCTs can be entrusted to capable research institutions, imposing confidentiality

5. System for Non-Disclosure of Selected Patent Applications (Chapter V)

In order to prevent disclosure or divulgence of inventions that are likely to be detrimental to national security through patent procedures, as well as to ensure rights under the Patent Act without compromising national security, the Act introduces measures to suspend publication of patent applications by security designations, and to restrict filling of such an application in a foreign country, etc.

Review from a Perspective of Technology Fields, etc. (primary review)

- The Japan Patent Office sends patent applications that include inventions in specified technology fields to the Cabinet Office.

Security Review (secondary review)

Review from perspectives of:

1. the risk of detrimental impact to the security of the nation and its citizens; and
2. impact on the industrial development due to non-disclosure of the invention, etc.

Security Designation

- Effect of the designation: Prohibition on application withdrawal, requirement of permission to work a patent, prohibition on disclosure, requirement of appropriate management of information, etc.

Foreign Filing Restrictions

Compensa-tion

Effective Date

- Within 6 months to within 2 years after promulgation (18 May 2022) (enforced in stages)

Source: Cabinet Office Government of Japan (CAO) & Ministry of Economy, Trade and Industry (METI)

6.4 Appendix D: Singapore

Personal Data Protection Act (PDPA)

The Personal Data Protection Act (PDPA) is Singapore's law that protects personal data, regulates its use by organizations, and includes a Do Not Call (DNC) Registry, allowing individuals to opt out of receiving unsolicited telemarketing messages. The PDPA covers personal data in both electronic and non-electronic formats. It generally does not apply to any individual acting on personal/domestic basis, any individual acting in his/her capacity as an employee with an organization, public agency data, and business contact information.

The PDPA mandates that organizations must comply with 11 main data protection obligations when collecting, using, or disclosing personal data. These include the following obligations: Accountability, Notification, Consent, Purpose Limitation, Accuracy, Protection, Retention Limitation, Transfer Limitation, Access and Correction, Data Breach Notification, and Data Portability.

The 2022 amendments to the PDPA have increased financial penalties for data breaches and enhanced the enforcement powers of the PDPC. The financial penalties for breaches have a cap of up to 10% of the organization's annual turnover in Singapore, in any other case, S$1 million, whichever is higher.

The Personal Data Protection Act (PDPA) is Singapore's law that protects personal data, regulates its use by organizations, and includes a Do Not Call (DNC) Registry, allowing individuals to opt out of receiving unsolicited telemarketing messages.

Objectives of the PDPA: The PDPA aims to protect personal data, ensure its legitimate use by organizations, prevent misuse, maintain trust, and position Singapore as a trusted business hub.

Scope of the PDPA: The PDPA covers personal data in both electronic and non-electronic formats. It generally does not apply to personal/domestic use, employee data, public agency data, and business contact information.

Data Protection Obligations: The PDPA mandates that organizations must comply with 11 main data protection obligations when collecting, using, or disclosing personal data. These include:

- Accountability Obligation: Ensure compliance with PDPA; provide data protection policy information; designate and publicize a Data Protection Officer (DPO).
- Notification Obligation: Inform individuals about the purposes for collecting, using, or disclosing their personal data.
- Consent Obligation: Collect, use, or disclose data only with consent; allow withdrawal of consent with reasonable notice and cease data use upon withdrawal.
- Purpose Limitation Obligation: Use data only for reasonable and consented purposes; do not require consent beyond what is necessary for the service/product.
- Accuracy Obligation: Ensure personal data is accurate and complete, especially if used for decisions affecting individuals or shared with others.
- Protection Obligation: Implement reasonable security measures to protect personal data from unauthorized access, use, or disclosure.
- Retention Limitation Obligation: Stop retaining or properly dispose of personal data when no longer needed for business or legal purposes.
- Transfer Limitation Obligation: Transfer personal data internationally only if protection standards match PDPA, unless exempted by PDPC.

- Access and Correction Obligation: Provide access to personal data and its use history upon request; correct errors and notify relevant parties of corrections.
- Data Breach Notification Obligation: Assess data breaches; notify PDPC and affected individuals if the breach likely causes significant harm or is of significant scale.
- Data Portability Obligation: Transmit an individual's data to another organization upon their request in a commonly used machine-readable format.

Compliance and Enforcement: The 2022 amendments to the PDPA have increased financial penalties for data breaches and enhanced the enforcement powers of the PDPC. The financial penalties for breaches have a cap of up to 10% of the organization's annual turnover in Singapore if it exceeds S$10 million.

The Charter of Trust

Protecting the digital world of tomorrow

About the Charter of Trust

The Charter of Trust is a non-profit alliance of leading global companies and organisations working across sectors to make the digital world of tomorrow a safer place. It was founded in 2018 at the Munich Security Conference to enhance cybersecurity efforts and foster digital trust in the face of an increasingly complex and severe cyber threat landscape.

A unique initiative underpinned by 10 principles fundamental to a secure digital world, the Charter of Trust is working to protect our increasingly digitized world and build a reliable foundation on which trust and digital innovation can flourish. It contributes to the development of effective cybersecurity policies that strengthen global cybersecurity posture and provides expertise on topics including AI, security by default, supply chain security, and education.

Objectives

The Charter of Trust seeks to harmonize cybersecurity approaches and address cybersecurity challenges from a holistic, ethical and fair perspective. The alliance is collaborating across industries to cultivate, advocate, and enhance global cybersecurity standards. By fostering widespread awareness and sharing expertise, it ensures a cohesive approach to security that enables seamless global interoperability.

Key principles

The work of the Charter of Trust is underpinned by 10 principles fundamental to a secure digital world:

1. Ownership for cyber and IT security
2. Responsibility throughout the digital supply chain
3. Security by default
4. User-centricity
5. Innovation and co-creation
6. Education
7. Cyber-resilience through conformity and certification
8. Transparency and response
9. Regulatory framework
10. Joint initiatives

Contact

Point of contact: contact@charteroftrust.info

Contributors

- ATOS SE
- CERT-In
- Eviden
- IBM Corporation
- Infineon Technologies AG
- Microsoft Corporation
- Mitsubishi Heavy Industries, Ltd.
- NXP Semiconductors N.V.
- Robert Bosch GmbH
- Siemens AG
- TÜV SÜD AG