Malaysia Data Security Governance Reference Book

Unleashing the Value of Reliable Data

Published by:

PIKOM

Supported by:

MDEC™

CyberSecurity MALAYSIA

Contents

Foreword

As the Chairman of the National Tech Association of Malaysia, I am pleased to introduce the Malaysia Data Security Governance Reference Book that PIKOM has developed together with Malaysia Digital Economy Corporation and Cybersecurity Malaysia.

The document provides guidelines to improve Malaysia's data security governance maturity and efficiency and is a valuable resource for organizations of all sizes in Malaysia. It covers a wide range of topics, including data sovereignty, key standards, and global advanced practices as well as recommendations and ways forward.

The Malaysia Data Security Governance Reference Book is an essential resource for organizations that want to protect their data and build trust with their customers. I encourage all organizations in Malaysia to adopt the principles and practices outlined in this book.

I would like to thank the Malaysia Digital Economy Corporation and Cybersecurity Malaysia for their support and the team of experts who worked on this project. Their dedication and hard work have made this book a valuable resource for organizations in Malaysia as we moved towards achieving the goals set out in the Malaysia Digital Economy Blueprint, to successfully transform Malaysia into a digitally-driven, high-income nation and a regional leader in the digital economy.

I hope that this book will help to raise awareness of the importance of data security in Malaysia. By working together, we can create a more secure and trustworthy digital environment for everyone.

Sincerely,

ONG CHIN SEONG
PIKOM CHAIRMAN

Foreword

On behalf of the Malaysia Digital Economy Corporation (MDEC), I would like to thank the National Tech Association of Malaysia for their collaboration on this project. Their expertise and insights have been invaluable in ensuring that this book is a vital resource for organisations in Malaysia.

As the nation's digital economy continues to grow, it becomes more apparent that data fuels the technology around us. Ensuring data security is paramount. This necessity catalyses an immense acceleration in key areas such as cybersecurity, and MDEC is actively focusing on attracting digital investment into Malaysia through this sector.

In line with these technological advancements, I firmly believe that the development of Malaysia Data Security Governance Reference Book is timely for Malaysia's thriving digital economy. This comprehensive reference book is a testament to our collective commitment to building a secure digital ecosystem. It is a valuable resource for organisations of all sizes, and it will aid in amplifying awareness on the significance of data security in Malaysia.

I encourage all organisations in Malaysia to refer and adopt the principles and practices outlined in this book. With your support, we can contribute to the establishment of an enhanceddigital ecosystem, fostering greater confidence and integrity, while strengthening the foundations of Malaysia's burgeoning digital economy.

Sincerely,

TS. MAHADHIR AZIZ
CHIEF EXECUTIVE OFFICER,
MALAYSIA DIGITAL ECONOMY CORPORATION (MDEC)

1 Normative references

The following normative references are indispensable for the application of this Malaysia Data Security Governance Reference Book. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

See Annex A.

2 Abbreviations

AI	Artificial intelligence
ML	Machine learning
RPA	Robotic process automation
CSPs	Cloud service providers
CSCs	Cloud Service Customers
GDPR	General Data Protection Regulation
IoT	Internet of Things
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
CSA CCM	Cloud Security Alliance Cloud Controls Matrix
CIPS	Cloud Infrastructure and Platform Services Market
SaaS	Application Software as a Service Market
IaaS	Infrastructure as a Service Market
PaaS	Platform as a service
ABS	Association of Banks in Singapore
OSPAR	Outsourced Service Provider’s Audit Report
PCI DSS	Payment Card Industry (PCI) Data Security Standards (DSS)
PCI 3DS	Payment Card Industry (PCI) 3-D Secure specification(3DS)
CIS Controls	CIS Critical Security Controls

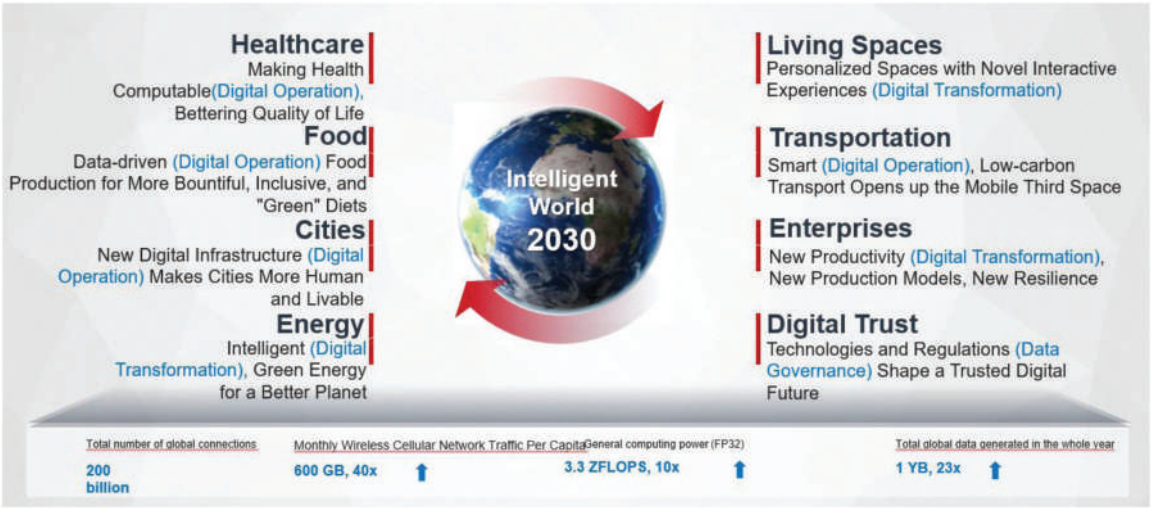
3 Outlook for Intelligent World 2030

We are making strides towards an intelligent world. When looking ahead to 2030, we hope that the future will bring improved quality of life, sustainable and green diets, and more comfortable living spaces. We also look forward to the end of traffic congestion and pollution in cities, fully green energy, and a wide range of new digital services. We dream of robots that can do repetitive and dangerous work for us so that we can devote more time and energy to more valuable, creative work, and to our personal interests. These are the goals that drive exploration in every industry.

We have examined the prospects for the intelligent world over the next decade by analyzing macro trends in healthcare, food, living spaces, transportation, cities, enterprises, energy, and digital trust. We believe in the infinite possibilities of the intelligent world, but constant collaboration and exploration among many different industries will be required to build a better future.

Digital technology, digital transformation, digital operations and data governance can better meet the requirements of the eight dimensions of human social development in the future intelligent world: healthcare, food, cities, energy, living spaces, transportation, enterprise, and digital trust.

Figure 1 Intelligent World 2030



- **Outlook for Healthcare: Making Health Computable, Bettering Quality of Life**
  By 2030, sensitive biosensors will be in widespread use, and massive amounts of health data will be stored on the cloud, making health computable. People will be able to proactively manage their health, shifting focus from treatment to prevention. Driven by technologies such as IoT and AI, personalized treatments will become a reality. Portable medical devices will enable people to access coordinated telemedicine services from the comfort of their homes.

- **Outlook for Food: Data-driven Food Production for More Bountiful, Inclusive, and "Green" Diets**
  By 2030, we will be producing visualized data graphs, which will make precision farming possible. Collecting data will enable us to control factors affecting crop growth, such as temperature and humidity, so that we can build vertical farms unaffected by the uncertainties of climate and weather. 3D printing technologies are also introducing the possibility of artificial meat designed according to taste and dietary requirements. By 2030, we will be building more resilient and sustainable food systems and relying on firm data rather than the vagaries of the heavens.

- **Outlook for Living Spaces: Personalized Spaces with Novel Interactive Experiences**
  By 2030, we will no longer have to live with clutter. We will manage our possessions with a digital catalog powered by a 10-gigabit network, holograms, and other technologies. Automatic delivery systems will bring household items from shared warehouses to our doors whenever we need them. Intelligent management systems that control our physical surroundings for automatic interactions will mean that the buildings where we live and work may produce net zero carbon. Next-generation IoT operating systems will enable people to live and work in adaptive environments that understand their needs.

- **Outlook for Transportation: Smart, Low-carbon Transport Opens up the Mobile Third Space**
  In 2030, the transport system will see innovations across many different dimensions. Vehicles using green energy and controlled by autonomous driving technology will provide us with a mobile third space. Electric vertical take-off and landing (eVTOL) aircraft will make emergency rescue faster, reduce the costs of delivering emergency medical supplies, and may even change how people commute. Mobility solutions will be efficient, customized, and shared, meaning that vehicles will be used much more consistently and travel will become greener.

  All of these will require secure and stable autonomous driving algorithms; cost-effective, reliable sensors; high-speed, stable space-air-ground integrated networks; and a central brain with massive computing power for traffic management. These technologies will be indispensable for developing connected, autonomous, shared, and electric vehicles that deliver a low-carbon transport experience.

- **Outlook for Cities: New Digital Infrastructure Makes Cities More Human and Livable**
  The spread of new digital infrastructure will make for better management of the urban environment, with more efficient use of resources and more effective city governance. Centralized digital platforms for government processes and services will make government services user-friendly and easier to access. This will help create more comfortable and livable cities.

- **Outlook for Enterprises: New Productivity, New Production Models, New Resilience**
  By 2030, digital transformation will have brought a new wave of modernization to enterprises. They will use more productive machines, such as collaborative robots and autonomous mobile robots. New business models will be more people-centric, with increased flexibility in manufacturing, logistics, and other activities. Digitalization will help companies interweave and graphically monitor their supply chains for better resilience in the face of dynamic market environments.

- **Outlook for Energy: Intelligent, Green Energy for a Better Planet**
  Energy will be greener and more intelligent in 2030. Power plants will be generating electricity from renewable energy sources in lakes and near-shore marine areas. An “energy Internet” will emerge, with digital technologies connecting generation-grid-load-storage, including virtual power plants and an energy cloud. Zero-carbon data centers and zero-carbon telecom towers could possibly become a reality.

- **Outlook for Digital Trust: Technologies and Regulations Shape a Trusted Digital Future**
  In 2030, digital trust will be a basic requirement for our social infrastructure. We will need a combination of technical and organizational measures: blockchain, AI fraud detection, and privacy-enhancing computation. This will need to be combined with personal privacy/information protection, cloud service security and data security governance regulations such as the General Data Protection Regulation (GDPR), CSA CoC for GDPR Complacent Privacy Framework, CSA CCM,ISO series standards. Used together, these measures will deliver an intelligent world with digital trust.

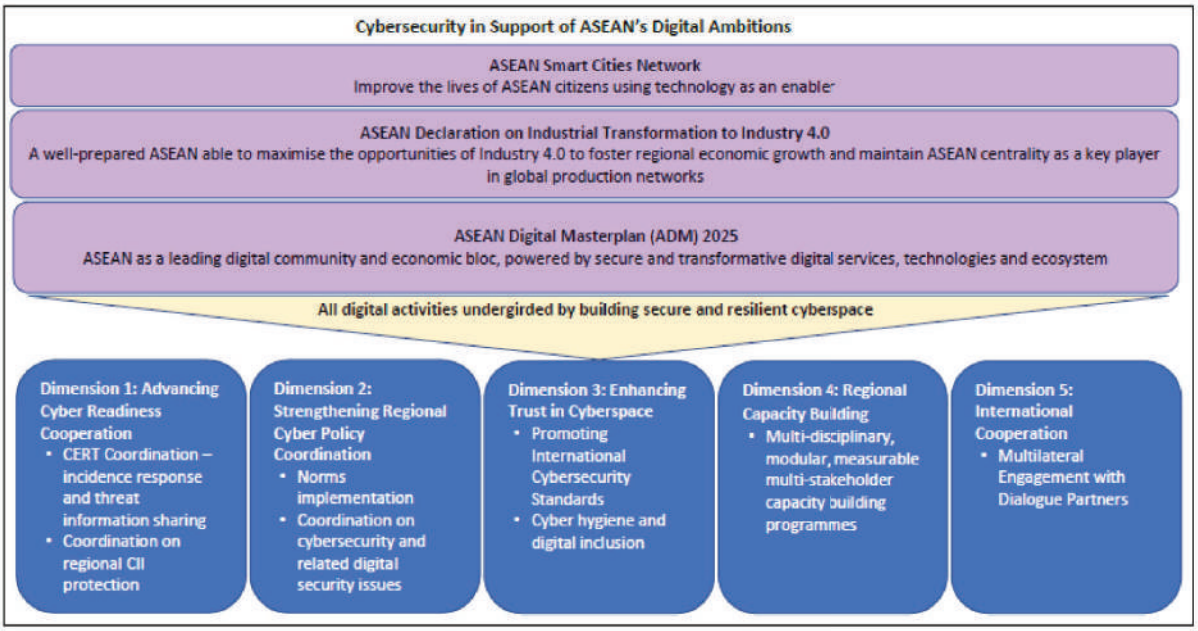
4 Recap of OBJECTIVE OF ASEAN-Cybersecurity-STRATEGY[2]

In view of the changes in the cyber and digital domain, the overarching objective of developing a new ASEAN Cybersecurity Cooperation Strategy is to update ASEAN's approach, while continuing to build on existing achievements. This update will guide the creation of a safer and more secure cyberspace in the ASEAN region. A secure, interoperable, and resilient cyberspace in the ASEAN region undergirds and enables ASEAN's digital ambitions. These digital ambitions are reflected in numerous initiatives such as the ASCN, the ASEAN Declaration on Industrial Transformation to Industry 4.0, and the ADM 20254. These ambitions can be curtailed by the greater attack surface resulting from increased digital interconnectedness, complexity of increasingly interrelated cyber and digital issues, and increasingly sophisticated cyberattacks.

To support ASEAN's digital economy and ambitions, the 2021 – 2025 Strategy seeks to support the establishment of a rules-based multilateral order for cyberspace, one that is open, secure, stable, accessible, interoperable and peaceful; built through the application of voluntary, non-binding norms of responsible State behaviour, confidence building measures, and coordinated capacity-building by enhanced cooperation within ASEAN and with our ASEAN Dialogue Partners.

The 2021 – 2025 Strategy builds on the foundation laid by the first Strategy in incident response, CERT and capacity building cooperation, and considers the rapid cybersecurity landscape changes for the purpose of creating a safe and secure cyberspace in the ASEAN region. It contains five dimensions of work:
(1) Advancing Cyber Readiness Cooperation;
(2) Strengthening Regional Cyber Policy Coordination;
(3) Enhancing Trust in Cyberspace;
(4) Regional Capacity Building; and
(5) International Cooperation.

Figure 2: Cybersecurity in Support of ASEAN's Digital Ambitions



[2] ASEAN-Cybersecurity-Cooperation-Paper-2021-2025, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

5 Regarding data sovereignty, cyber security, data security and privacy

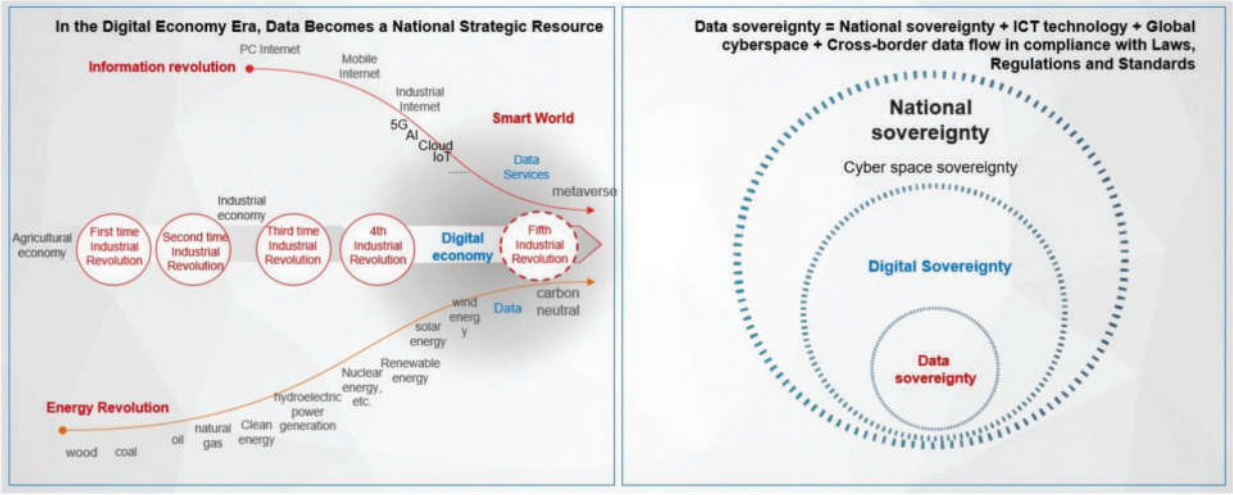
5.1 Data Sovereignty

The definition of sovereignty applies only to countries, while cyber (space) sovereignty, digital sovereignty, and data sovereignty impose sovereignty restrictions on countries' information assets from different dimensions, emphasizing the independence of national data and related facilities.

Data sovereignty = National sovereignty + ICT technologies + Global cyberspace + cross-border data transfer in compliance with laws, regulations and standards.

Each country has its own concept of digital sovereignty. Any enterprise, institution, organization, and individual must firmly support national data sovereignty, as well as national digital sovereignty strategy and requirements. At the same time, we call on cross-border data transfer in compliance with laws, regulations and standards.

Figure 3: Data sovereignty



Source:ASEAN secretariat working group.,2022Q4

- **National sovereignty:** refers to the most important attribute that distinguishes a country from other social groups. It is the inherent supreme power of a country at home and its independent right at the international level.

  National sovereignty is the core attribute of national security, and ensuring the security of national sovereignty is the core task and mission of national security.

  Scope: land, sea, sky, and cyberspace (the fourth space), including independence, jurisdiction, defense, and equality.

- **Internet sovereignty or cyber sovereignty:** It is the natural extension and expression of national sovereignty in cyberspace.

  Internally, cyber sovereignty refers to the independent development, supervision and management of the Internet affairs of the country.

  Externally, cyber sovereignty means protecting the cyber from outside intrusions and attacks.

- **Digital sovereignty:** A country has independent ownership and jurisdiction over its data, infrastructure, and digital technologies.

- **Cyber (space) sovereignty** is a general sovereignty, and various sovereignty claims in cyber space include "digital sovereignty", "technical sovereignty" and "data sovereignty". Cyber (space) sovereignty is the basis and framework of the other three sovereignty.

- **Data sovereignty:** A country's independent right to manage and utilize its own data, and free from interference and intrusion by other countries, including ownership and jurisdiction.

  The biggest characteristic: independence, namely, the right to completely control and freely manage the relevant data of the country, and the ability to eliminate any foreign interference, to guarantee the security and stability of the data of the country against other countries, is closely related to national security.

  Data types: important identification data, important service data, important audit data, important configuration data, important video data, and important personal information.

- **Data right** refers to the right to possess, dominate, use, benefit, and disposal of data property. From the perspective of implementing subject, data right can be divided into two aspects: public right and private right according to different subject types.

  The data public right is the platform party, and the platform party independently manages and uses the customer transaction data on the transaction platform.

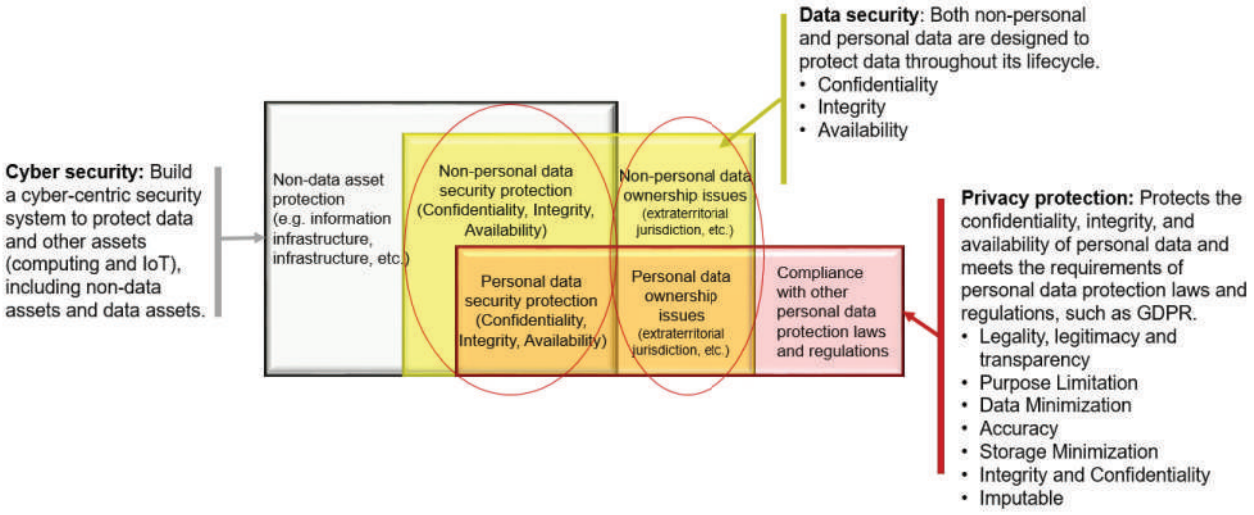
5.2 Comparison of Cyber security, Data security and Privacy protection

» Cyber security: Build a cyber-centric security system to protect data and other assets (computing and IoT), including non-data assets and data assets.

» Data security: Both non-personal and personal data are designed to protect data throughout its lifecycle.
- Confidentiality
- Integrity
- Availability

» Privacy protection: Protects the confidentiality, integrity, and availability of personal data and meets the requirements of personal data protection laws and regulations, such as GDPR.
- Legality, legitimacy and transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Minimization
- Integrity and Confidentiality
- Imputable

Figure 4: Comparison of Cyber security and Privacy protection



» **Cyber security**: Cyberspace security focuses on network resources and environments. It ensures the security of networks and access network devices, and finally ensures data security.

» **Data security**: Focus on security and compliance throughout the data lifecycle, and may involve extra-domain effectiveness.

» **Privacy protection**: Focus on the use and governance of personal data. For example, policies are in place to ensure that consumers' personal information is collected, shared and used in an appropriate manner.

» **Data security**: The focus is on protecting data against malicious attacks and using stolen data for profit.

Understanding from two perspectives,

» **Economic development perspective**: Implement fine-grained control based on data classification, ensure data security, compliance, use, and transfer, and ultimately create value.

» **Cyber security perspective**: Based on the system and network, establish region isolation and division of security domains, transform data systems into security sandboxes, and protect data against attacks and data leakage.

5.3 Data security

Growing internet connections and the digitization of the global economy have led to a rapid increase in the collection, use and cross-border transmission of data, a trend that continues to accelerate. Not only for large multinational technology companies, but also for micro, small and medium-sized businesses, workers and consumers in all sectors of the economy, the rules of data governance need to match the rapid and healthy development of the digital economy.

Reliable data can raise living standards, create jobs, increase government data services taxes, and connect people in meaningful ways to support important research and applications in multiple areas, and foster innovation and entrepreneurship.

In the digital economy era, data has become a strategic resource of a country. Governments can formulate data strategies and governance rules to safeguard national data sovereignty and improve national competitiveness in the digital economy.

Data governance involves data sovereignty, digital sovereignty, digital transformation, digital operation, cyber security, and data security. It involves multiple stakeholders, including countries, governments, enterprises, industry organizations and consumers. Data governance more directly faces the balancing and gambling between openness and conservativeness, multilateralism and isolation, economic development and cyber security, and has a profound impact on the global political and economic landscape.

The ultimate purpose of data security governance is to create value. The overall strategy is unleashing the value of reliable data. Governments shall take the lead in building a multi-stakeholder collaborative governance model that adapts to the rapid development of the digital economy by cloud as a foundation. Countries, governments, enterprises, industry organizations, and consumers should participate more in global data governance communication and collaboration to build rules and share values.

In implementing a data service, various countries have addressed several important issues that are to be considered in selecting key cloud service security governance. These include Data sovereignty, personal privacy/information protection, data classification and government guidelines, standards and global countries best practices for the implementation of a data service.

5.4 Security and Privacy

Maintaining security and protecting the right to privacy is another important issue. There are several types of data contained in the public sector's database, including personal data and not personal data. At the same time, this may be important government data that if it is leaked or dropped would cause serious damage. Thus, as can be seen, the data hierarchy is also classified. Keeping that data secure; in addition to maintaining the privacy of the personal data of those involved, protects the public interest or the benefit of the public sector that would conduct its duties and not be damaged by the fact that the data was leaked. Therefore, the use of Cloud computing is part of the driving force of the public sector's duties. As such, there is a need to address the security issues of data processing that takes place in the Cloud to be standardized and sufficient to preserve sensitive data. However, as mentioned above, certain types of highly sensitive data according to some countries' policies or laws may have restrictions on uploading data to the Cloud, or it can be uploaded to the cloud, but there is a requirement that the data must be placed in a system within the boundaries of that country, or as it known as Data Residency or Data Localization.

The protection of personal data is another important consideration, especially the case in the EU's General Data Protection Regulation (GDPR). Cloud service providers usually have the status of data processors that have been assigned by the data controller. They must also comply with the privacy laws, even if they are not located in Europe. There must also be a contract for processing the content of the personal data as required by law. In addition, there are other legal duties, e.g., European law regulates the transfer of data outside the territory of a member state in which there must be a process to verify that the destination has adequate personal data protection measures. Cloud service providers must also be able to properly comply with the privacy laws.

The security requirements, including the protection of that personal data, are often the requirements and considerations used in the procurement of Cloud service providers. Thus, this may be defined as a qualification in procurement, contract specification, or even having the qualifications of a Cloud service provider to have accreditation. This would be able to provide Cloud services to public sector agencies as well.

5.5 Data Classification

Although Cloud services have many of the advantages mentioned above, even on the issue of security, one concern for using Cloud services is the importance of data that can be stored or processed in the Cloud. This issue raises the question of what kind of data can be uploaded to the Cloud. Another question may be about obtaining important data regarding the performance of public sector duties, or even personal data that can be uploaded into the Cloud of any service provider. In following the above issues, classification of the data types and their implementation to access the specific Cloud system is therefore a key issue and is part of the Cloud computing policy or strategy.

6 Key Standards and Global Advanced Practices

There is a variety of security standards both in Malaysia and around the world. Below, we list some well-established industry standards, such as standards of strategic construction, standards of personal privacy/ information protection, standards of cloud service security, and standards of system management and organizational governance and so on.

6.1 Key Standards for Digital Application

6.1.1 AR/VR

AR/VR enhances the efficiency of the Digital Experience for the benefit of learning and simulation for various industries.

» **ISO/IEC 18038:2020 Information technology — Computer graphics, image processing and environmental representation— Sensor representation in mixed and augmented reality**[3] defines the framework and information reference model for representing sensor-based 3D mixed-reality worlds. It defines concepts, an information model, architecture, system functions, and how to integrate 3D virtual worlds and physical sensors in order to provide mixed-reality applications with physical sensor interfaces. It defines an exchange format necessary for transferring and storing data between physical sensor-based mixed-reality applications.
ISO/IEC 18038:2020 specifies the following functionalities:
a) representation of physical sensors in a 3D scene;
b) definition of physical sensors in a 3D scene;
c) representation of functionalities of each physical sensor in a 3D scene;
d) representation of physical properties of each physical sensor in a 3D scene;
e) management of physical sensors in a 3D scene;
f) interface with physical sensor information in a 3D scene.

» **ISO/IEC 18039:2019 Information technology — Computer graphics, image processing and environmental data representation — Mixed and augmented reality (MAR) reference model**[4] defines the scope and key concepts of mixed and augmented reality, the relevant terms and their definitions and a generalized system architecture that together serve as a reference model for mixed and augmented reality (MAR) applications, components, systems, services and specifications. This architectural reference model establishes the set of required sub-modules and their minimum functions, the associated information content and the information models to be provided and/or supported by a compliant MAR system.

» **IEEE P2048 Standard for Augmented Reality on Mobile Devices: General Requirements for Software Framework, Components, and Integration**[5] specifies the general technical framework, components, integration, and main business processes of augmented reality systems applied to mobile devices, and defines its technical requirements, including functional requirements, performance requirements, safety requirements and corresponding test methods. This standard is applicable to the design, development, and management of augmented reality enabled applications or features of applications on mobile devices.

» **IEEE P3141 Standard for 3D Body Processing**[6] addresses the anthropometric and topo-physiological attributes that contribute to the quality of experience of 3D body processing, as well as identifying and analyzing metrics and other useful information, as well as data relating to these attributes. The standard defines a harmonized framework, suite of objective and subjective methods, tools, and workflows for assessing 3D body processing quality of experience attributes. The standard specifies and defines methods, metrics, and mechanisms to facilitate interoperability, communication, security and trusted operation of 3D body processing technologies. This includes quality of output of devices (such as sensors and/or scanners), digitization, simulation and modeling, analytics and animation, data transmission and visualization in the 3D body processing ecosystem, the ecosystem being in the near environment that interacts with the body.

[3] ISO/IEC 18038:2020 Information technology — Computer graphics, image processing and environmental representation— Sensor representation in mixed and augmented reality, https://www.iso.org/standard/70720.html
[4] ISO/IEC 18039:2019 Information technology — Computer graphics, image processing and environmental data representation — Mixed and augmented reality (MAR) reference model, https://www.iso.org/standard/30824.html
[5] IEEE P2048 Standard for Augmented Reality on Mobile Devices: General Requirements for Software Framework, Components, and Integration, https://standards.ieee.org/ieee/2048.101/10390/
[6] IEEE P3141 Standard for 3D Body Processing, https://standards.ieee.org/ieee/3141/10825/

6.1.2 IoT

IoT facilitates applications to increase the ability to connect data between devices quickly in both life and industry.

» **ISO/IEC 21823-1:2019 Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework**[7] provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems. This document enables IoT systems to be built in such a way that the entities of the IoT system are able to exchange information and mutually use the information in an efficient way. This document enables peer-to-peer interoperability between separate IoT systems. This document provides a common understanding of interoperability as it applies to IoT systems and the various entities within them.

» **ISO/IEC 21823-2:2020 Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability**[8] specifies a framework and requirements for transport interoperability, in order to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system.

» **ISO/IEC 21823-3:2021 Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability**[9] provides the basic concepts for IoT systems semantic interoperability, as described in the facet model of ISO/IEC 21823-1, including: – requirements of the core ontologies for semantic interoperability; – best practices and guidance on how to use ontologies and to develop domain-specific applications, including the need to allow for extensibility and connection to external ontologies; – cross-domain specification and formalization of ontologies to provide harmonized utilization of existing ontologies; – relevant IoT ontologies along with comparative study of the characteristics and approaches in terms of modularity, extensibility, reusability, scalability, interoperability with upper ontologies, and so on, and; – use cases and service scenarios that exhibit necessities and requirements of semantic interoperability.

» **ISO/IEC 21823-4:2022 Internet of things (IoT) — Interoperability for IoT systems — Part 4: Syntactic interoperability**[10] specifies the IoT interoperability from a syntactic point of view. In ISO/IEC 21823-1: Framework [2], five facets are described for IoT interoperability, i.e. transport, semantic, syntactic, behavioural and policy.

» **ETSI SR 003 680 Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach**[11] intends to be a high-level document for the general public and is not specifically addressing a technical audience (e.g. designers, developers, etc.). It is introducing, in a relatively non-technical manner, to some of the main issues that individuals and organizations should address when they face the development of an IoT system. A strong emphasis is put on interoperability, security, privacy and standards in support.

» **ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements**[12] specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services.

[7] ISO/IEC 21823-1:2019 Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework, https://www.iso.org/standard/71885.html
[8] ISO/IEC 21823-2:2020 Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability, https://www.iso.org/standard/80986.html
[9] ISO/IEC 21823-3:2021 Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability, https://www.iso.org/standard/83752.html
[10] ISO/IEC 21823-3:2021 Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability, https://www.iso.org/standard/84773.html
[11] ETSI SR 003 680 SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition;A Concrete Approach, https://www.etsi.org/deliver/etsi_sr/003600_003699/003680/01.01.01_60/sr_003680v010101p.pdf
[12] ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

» **OWASP IoT verification standard**[13] is a community effort to establish a framework of security requirements for Internet of Things (IoT) applications. The requirements provided by the ISVS can be used at many stages during the product development life cycle including design, development, and testing of IoT applications.IoT applications are often composed of many interconnected applications that together form a complex ecosystem. Securing an IoT application thus boils down to securing the ecosystem. The ISVS, therefore, specifies security requirements for embedded applications and the IoT ecosystem in which these reside while referring to existing industry-accepted standards as much as possible.

6.1.3 Biometrics

Biometrics is used for highly secure identification and verification, increasing the security of electronic transactions or logging into digital services

» **ISO/IEC JTC 1/SC 37 Biometrics**[14] standardizes generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects. Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification.

6.1.4 Healthcare

Aim to enhance the security of medical device software and medical devices.

» **ISO 62304 Medical device software — Software life cycle processes**[15] defines the life cycle requirements for medical device software. The set of processes, activities, and tasks described in this standard establishes a common framework for medical device software life cycle processes.

» **ISO 14971 Medical devices — Application of risk management to medical devices**[16] specifies terminology, principles and a process for risk management of medical devices, including software as a medical device and in vitro diagnostic medical devices. The process described in this document intends to assist manufacturers of medical devices to identify the hazards associated with the medical device, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls.

6.2 Key Standards for Digital Technology

6.2.1 AI/ML/RPA

AI/ML/RPA Is integrated with digital services to add more automated processes that replace work, increase analytics, and make accurate decisions.

» **ISO/IEC JTC 1/SC 42 (Series) Artificial intelligence**[17]
- Serve as the focus and proponent for JTC 1's standardization program on Artificial Intelligence
- Provide guidance to JTC 1, IEC, and ISO committees developing Artificial Intelligence applications

» **ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence**[18] surveys topics related to trustworthiness in AI systems, including the following:
- approaches to establish trust in AI systems through transparency, explainability, controllability, etc.;
- engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and
- approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems.

[13] OWASP IoT verification standard, https://owasp.org/www-project-iot-security-verification-standard/
[14] ISO/IEC JTC 1/SC 37 Biometrics, https://www.iso.org/committee/313770.html
[15] ISO 62304 Medical device software — Software life cycle processes, https://www.iso.org/standard/38421.html
[16] ISO 14971 Medical devices — Application of risk management to medical devices, https://www.iso.org/standard/72704.html
[17] ISO/IEC JTC 1/SC 42 (Series) Artificial intelligence, https://www.iso.org/committee/6794475.html
[18] ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence, https://www.iso.org/standard/77608.html

6.2.2 Big Data

Big data is used to analyze digital data stored on the digital platform to increase business opportunities, customer satisfaction and reduce service risks.

» **ISO/IEC 20546:2019 Information Technology-Big Data-Overview and vocabulary**[19] provides a set of terms and definitions needed to promote improved communication and understanding of this area. It provides a terminological foundation for big data-related standards and a conceptual overview of the field of big data, its relationship to other technical areas and standards efforts, and the concepts ascribed to big data that are not new to big data.

» **ISO/IEC TR 20547:2020 Information Technology-Big data reference architecture**[20] describes the framework of the big data reference architecture and the process for how a user of the document can apply it to their particular problem domain.

» **IEEE BDGMM BIG DATA GOVERNANCE AND METADATA MANAGEMENT: STANDARDS ROADMAP**[21] focuses on forming a community of interest from industry, academia, and government, intending to develop a standards roadmap for Big Data Governance and Metadata Management (BDGMM). The approach includes the following:
- Review BDGMM-related technology trends, use cases, general requirements, and reference architecture;
- Gain an understanding of what standards are available or under development that may apply to BDGMM;
- Perform standards, gap analysis, and document the findings; and
- Document vision and recommendations for future BDGMM standards activities that could have a significant industry impact.

6.2.3 Blockchain

Blockchain is used to support the work of a more digital system, e.g., IoT, e- Commerce as well as other applications with resource requirements.

» **ITU-T SG16 Q22 Multimedia aspects of distributed ledger technologies and e-services**[22] is considering:
- concepts, coverage, vision and use cases of e-services based on DLT;
- characteristics and requirements for e-services based on DLT;
- architectural framework and communication technologies of e- services based on DLT;
- analysis and evaluation of the current status of DLT and its maturity to support e-services;
- investigate the relations between DLT, digital fiat currencies and crypto tokens, including management, exchange and transactions, etc.;
- define general requirements and framework for DLT;
- research security and privacy aspects related to e-services based on DLT;
- examine means for extending online trust in the context of e-services using DLT;
- identify stakeholders with whom ITU-T could collaborate further on and potential collective actions and specific next steps.

» **TC590 National Technical Committee for Standardization of Blockchain and Distributed Accounting Technology**[23] is responsible for basic standards, business and application standards, process and method standards, trustworthiness and interoperability standards, and information security standards in the field of blockchain and distributed accounting technologies.

[19] ISO/IEC 20546:2019 Information Technology-Big Data-Overview and vocabulary, https://www.iso.org/standard/77608.html
[20] ISO/IEC TR 20547:2020 Information Technology-Big data reference architecture, https://www.iso.org/standard/71275.html
[21] IEEE BDGMM BIG DATA GOVERNANCE AND METADATA MANAGEMENT: STANDARDS ROADMAP, https://standards.ieee.org/wp-content/uploads/import/governance/iccom/bdgmm-standards-roadmap-2020.pdf
[22] ITU-T SG16 Q22 Multimedia aspects of distributed ledger technologies and e-services, https://www.itu.int/en/ITU-T/studygroups/2017-2020/16/Pages/q22.aspx
[23] TC590 National Technical Committee for Standardization of Blockchain and Distributed Accounting Technology, https://std.samr.gov.cn/search/orgDetailView?tcCode=TC590

6.2.4 Distributed Computing

Distributed Computing used to support the work of a more digital system, e.g., IoT, e- Commerce as well as other applications with resource requirements.

» **ISO/IEC TR 23188:2020 Information Technology-Cloud computing-Edge computing landscape**[24] examines the concept of edge computing, its relationship to cloud computing and IoT, and the technologies that are key to the implementation of edge computing. This document explores the following topics with respect to edge computing:
- concept of edge computing systems;
- architectural foundation of edge computing;
- edge computing terminology;
- software classifications in edge computing, e.g. firmware, services, applications;
- supporting technologies, e.g. containers, serverless computing, microservices;
- networking for edge systems, including virtual networks;
- data, e.g. data flow, data storage, data processing;
- management, of software, of data and of networks, resources, quality of service;
- virtual placement of software and data, and metadata;
- security and privacy;
- real time;
- mobile edge computing, mobile devices.

» **ISO/IEC JTC 1/SC 38 (Series) Cloud computing and distributed platforms**[25] serves as the focus, proponent, and systems integration entity on Cloud Computing, Distributed Platforms, and the application of these technologies. SC 38 provides guidance to JTC 1, IEC, ISO and other entities developing standards in these areas.

6.3 Key Standards for Digital Infrastructure

6.3.1 Mobile Network

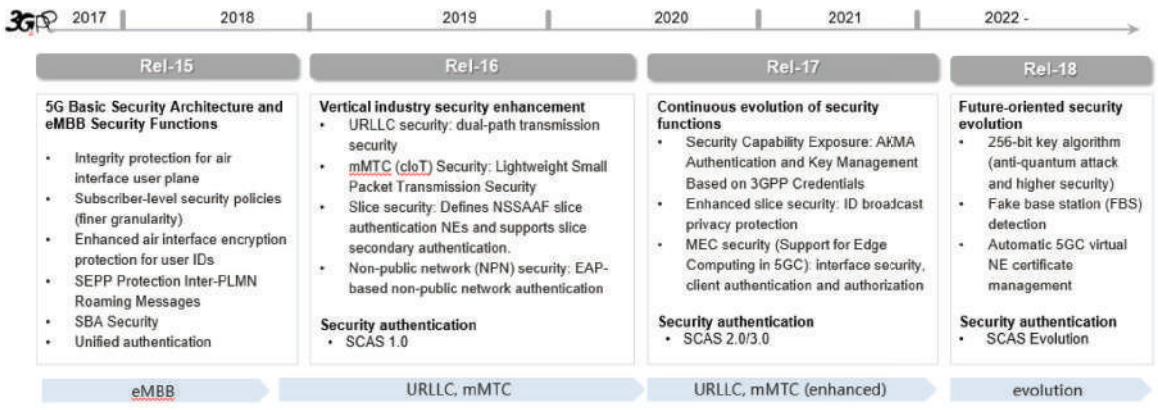
Aim to enhance the security of mobile network on operation security and deploy security.o

» **3GPP Release15/16/17/18**[26] uses a system of parallel “Releases” which provide developers with a stable platform for the implementation of features at a given point and then allow for the addition of new functionality in subsequent Releases.

5G faces security challenges and opportunities brought by new services, architectures, and technologies, as well as higher user privacy and protection requirements. The industry needs to understand the requirements of diversified scenarios and better define 5G security standards and technologies to address the associated risks.

The industry as a whole is working together to address new security risks faced by 5G architectures, technologies, and services, and address potential security challenges through unified 5G security standards, common 5G security concepts, and an agreed 5G security framework. During 2020, 111 companies (including their subsidiaries) from around the world sent technical experts to six SA3 meetings for the development of 5G security standards. The 3GPP SA3 Working Group has established 42 projects to analyze security threats and risks in various 5G scenarios. Project conclusions are being drawn gradually and implemented in security standards.

Figure 5: 3GPP SA3 Release



[24] ISO/IEC TR 23188:2020 Information Technology-Cloud computing-Edge computing landscape, https://www.iso.org/standard/74846.html
[25] ISO/IEC JTC 1/SC 38 (Series) Cloud computing and distributed platforms, https://www.iso.org/committee/601355.html
[26] 3GPP Release15/16/17/18, https://www.3gpp.org/specifications-technologies/releases

5G is an evolution of 3G and 4G technology that will enable new kinds of services. For example, ultra-reliable-low-latency communications (uRLLC) will make self-driving cars possible, and massive machine-type communications (mMTC) will underpin smart manufacturing. There is no fundamental difference between 5G and 4G network architecture; the core networks and radio access networks (RAN) are still separated. Moreover, 5G offers stronger guarantees regarding privacy and security protection than either 3G or 4G.

3GPP 5G standards have inherited existing 4G security standards and improved upon these standards. In terms of 5G, new security mechanisms and measures have been designed for cloud, mobile edge computing (MEC), and network slicing.

» **3GPP Study on security aspects of network slicing enhancement TS 33.813**[27]

» **GSMA 5G CKB**[28] is A comprehensive 5G Cybersecurity Knowledge Base to help stakeholders identify, map and mitigate risks.

As Mobile Network Operators (MNOs) around the globe introduce and launch 5G systems, communications networks will face new security threats and challenges. Understanding, mapping and mitigating these existing and upcoming security threats in an objective, speedy and effective manner has become essential.

To help operators and others in the 5G ecosystem, the GSMA has conducted a comprehensive threat analysis involving industry experts from across the eco-system including MNOs, vendors, service providers, and regulators, as well as collecting input from public sources such as 3GPP, ENISA and NIST, and mapped these threats to appropriate and effective security controls.

The GSMA has collated this analysis into a 5G Cybersecurity Knowledge Base to provide useful guidance on a range of 5G security risks and mitigation measures. The Knowledge Base aims to make available to GSMA members the combined knowledge of the 5G ecosystem to increase trust in 5G networks and make the interconnected world as secure as possible. Over time, the Knowledge Base will be enhanced and extended to respond to the evolving cybersecurity threat landscape.

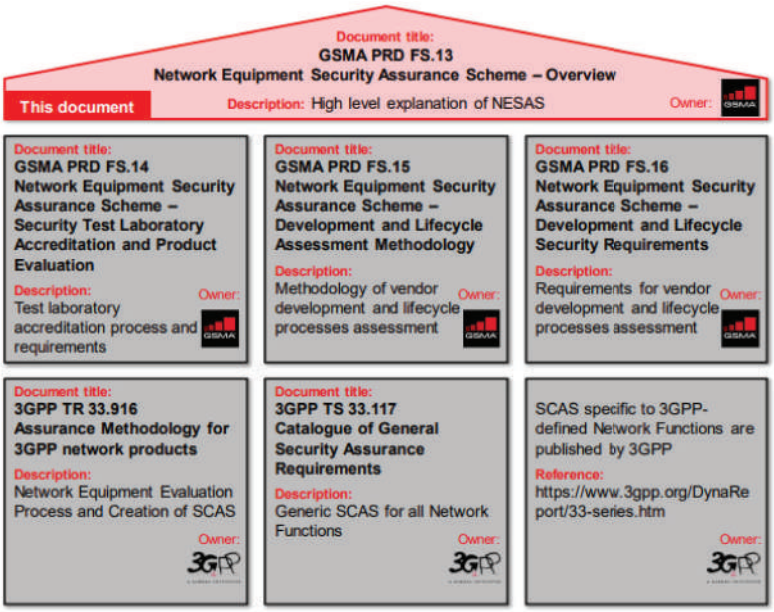
6.3.2 Wireless equipment

» **ITU-T work programme SG17 X.5G sec-guide**[29]
Connected IoT devices and mobile applications require wireless network access that is resilient, secure and able to protect individuals' privacy. The 5G communication system should be designed to meet these high-level requirements. There is a need for defining security framework for 5G communication system, which could be a concrete ground for developing further detailed technical Recommendations in 5G security subjects. ITU-T SG17 X.5G sec-guide provides security guidelines for 5G communication system. It identifies all components related to security of 5G communication system. It describes generic 5G architecture and its domain identifies threats to and provides security capabilities of each component, taking into account unique network features. ITU-T SG17 X.5G sec-guide is based on the 3GPP 5G security architecture.

» **NESAS|SCAS**[30] defines security requirements and an assessment framework for secure product Development and Product Lifecycle Processes, as well as security test cases for the security evaluation of network equipment. NESAS is of value to both operators and vendors, it is intended to be used alongside other mechanisms to ensure a network is secure, in particular an appropriate set of security policies covering the whole lifecycle of a network.

[27] 3GPP Study on security aspects of network slicing enhancement TS 33.813, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3541
[28] GSMA 5G CKB, https://www.gsma.com/security/5g-cybersecurity-knowledge-base/ Knowledge Base
[29] ITU-T work programme SG17 X.5G sec-guide, https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15006
[30] NESAS|SCAS, https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Figure 6: NESAS Overview v.2.0



6.3.3 Cloud service

Aim to standardize cloud service provider (CSPs), cloud service customer (CSCs), and provide the highest level of security for subscribers.

» **ISO/IEC 27017:2015**[31] is a practical rule for cloud service information security control established by the International Organization for Standardization (ISO) based on ISO 27001 (Information Security Management System) and ISO 27002 (Information Security, Network Security, and Privacy Protection - Information Security Control). ISO 27001 is a global information security standard. ISO 27002 provides best practice guidance applicable to the controls listed in Annex A of ISO 27001 to guide organizations' information security standards. ISO 27017 provides guidance specific to cloud service providers for the 37 control requirements in ISO 27002 and adds seven new control requirements to address the issues of operating in cloud services, allocation of authority and responsibility, security of information assets, security of the environment, and monitoring.

» **ISO/IEC 19790:2012**[32] the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems. This International Standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location). This International Standard specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level.

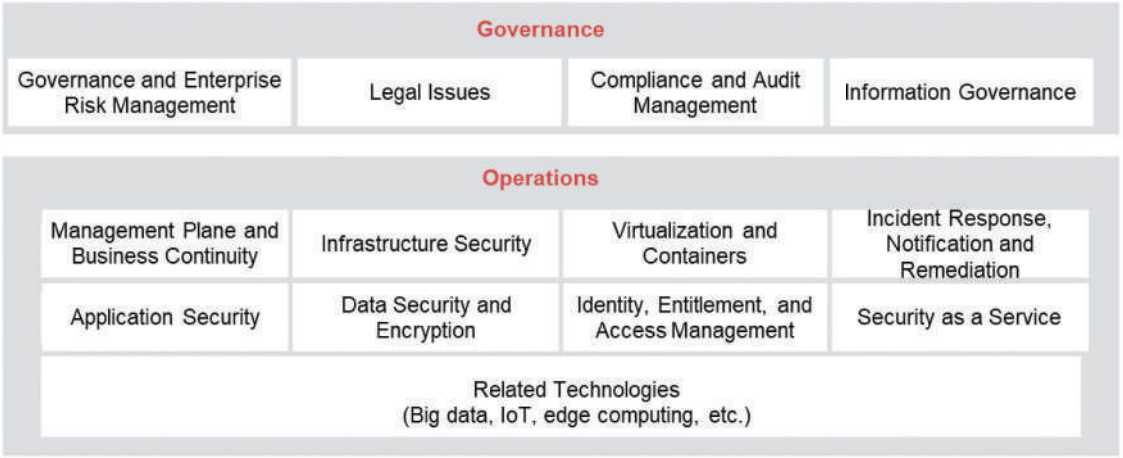
ISO/IEC 19790:2012 specifies security requirements specifically intended to maintain the security provided by a cryptographic module and compliance with this International Standard is not sufficient to ensure that a particular module is secure or that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected.

» **ISO/IEC 27034:2011**[33] provides guidance to assist organizations in integrating security into the processes used for managing their applications.ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.

» **CSA CCM :CSA**[34] developed the Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 in 2017, which expands the ISO/IEC 27001 ISMS and divides the cloud security framework into governance and operations based on CCM.

[31] ISO/IEC 27017:2015 Information Technology-Security Techniques-Code of practice for information security controls based on ISO/IEC 27002 for cloud services, https://www.iso.org/standard/43757.html
[32] ISO/IEC 19790:2012 Information technology-Security techniques-Security requirements for cryptographic modules, https://www.iso.org/standard/52906.html
[33] ISO/IEC 27034-1:2011 Information technology-Security techniques-Application security — Part 1: Overview and concepts, https://www.iso.org/standard/44378.html
[34] Cloud Controls Matrix (CCM), https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Figure 7: Cloud security architecture in CSA's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0



CCM v4 is composed of 197 control objectives that are structured in 17 domains covering all security aspects of cloud computing technology. It can be used as a tool for the systematic assessment of a cloud implementation, and provides guidance on which security controls should be implemented by which actor within the cloud supply chain.

CCM v4 aims to:

- Ensure coverage of requirements deriving from new cloud technologies (e.g., microservices, containers) and new legal and regulatory requirements especially in the privacy realm.
- Improve the auditability of the controls and provide better implementation and assessment guidance to organizations.
- Clarify the allocation of cloud security responsibilities within the shared responsibility model.
- Improve interoperability and compatibility with other standards.

CIS Controls lists 20 security controls, including Basic (6 controls), Foundation (10 controls), and Organizational (4 controls). From the perspective of "practice organization", implementation suggestions are proposed for organizations of different sizes, which are divided into IGs1 (family business), IGs2 (regional unit) and IGs3 (large enterprise).

» **CIS Critical Security Controls Version 8**[35]

The CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls v8 has been enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, Work-from-Home, and changing attacker tactics prompted the update and supports an enterprise's security as they move to both fully cloud and hybrid environments.

The CIS Critical Security Controls (CIS Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. The CIS Controls are a relatively short list of high-priority, highly effective defensive actions that provide a "must-do, do-first" starting point for every enterprise seeking to improve their cyber defense.

The CIS Controls were developed starting in 2008 by an international, grass-roots consortium bringing together companies, government agencies, institutions, and individuals from every part of the ecosystem (cyber analysts, vulnerability-finders, solution providers, users, consultants, policy-makers, executives, academia, auditors, etc.) who banded together to create, adopt, and support the CIS Controls. The expert volunteers who develop the Controls apply their first-hand experience to develop the most effective actions for cyber defense.

» **SOC 1/2/3**[36] :

An SOC report is an independent audit issued by a third-party audit institution based on relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the systems and internal controls of outsourced service providers. SOC reports are classified as SOC 1 (including Type I and Type II), SOC 2 (including Type I and Type II), or SOC 3.

[35] CIS Critical Security Controls Version 8, https://www.cisecurity.org/controls/v8
[36] SOC 1/2/3, https://www.aicpa.org/cpe-learning/course/soc--for-cybersecurity-certificate-program

- An SOC 1 report is intended to examine the controls related to financial reporting processes and is usually used by cloud customers and their independent auditors. SOC Type II reports provide more opinions on operational effectiveness than Type I reports to achieve related control objectives.
- An SOC 2 report focuses on the internal operations and compliance of an organization, including controls related to security, availability, process integrity, confidentiality, and privacy. An SOC Type I report demonstrates the design rationality of internal controls within the organization, and SOC Type II reports reflects the effectiveness of the implementation of the measures during the reporting period.
- An SOC 3 report is a summary version based on the SOC 2 Type II report and is available to the public.

» **NIST CSF**[37] **:**
The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was published in February 2014 as guidance for critical infrastructure organizations to better understand, manage, and reduce their cybersecurity risks. The CSF was developed in response to the Presidential Executive Order on Improving Critical Infrastructure Security, which was issued in February 2013. NIST released the CSF Version 1.1 in April 2018, incorporating feedback received since the original CSF release. An Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure signed in May 2017 requires US government agencies to use the NIST CSF or any successor document when conducting risk assessments for agency systems. Each agency head is required to produce a risk management report documenting cybersecurity risk mitigation and describing the agency's action plan to implement the CSF.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is an internationally recognized system for assessing information security. It provides guidance for organizations seeking to enhance cybersecurity. NIST CSF consists of standards, guidelines, and best practices to manage cybersecurity. They put forward an Identify, Protect, Detect, Response, Recovery (IPDRR) model, which helps organizations minimize risks before, during, and after a security incident.

6.3.4 Fixed network

Aim to enhance the security of fixed network equipment such as data com, router, switch and etc on equipment security.

» **The Common Criteria**[38] is to ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles; to improve the availability of evaluated, security-enhanced IT products and protection profiles; to eliminate the burden of duplicating evaluations of IT products and protection profiles; to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/ validation process for IT products and protection profiles.

6.4 Key Standards of Strategic Construction

» **ISO38505-1 Data Governance**[39] provides guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of data within their organizations by
- applying the governance principles and model of ISO/IEC 38500 to the governance of data,
- assuring stakeholders that, if the principles and practices proposed by this document are followed, they can have confidence in the organization's governance of data,
- informing and guiding governing bodies in the use and protection of data in their organization, and
- establishing a vocabulary for the governance of data.

ISO/IEC 38505-1:2017 can also provide guidance to a wider community, including:
- executive managers,
- external businesses or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies,
- internal and external service providers (including consultants), and
- auditors

[37] NIST CSF, https://www.nist.gov/cyberframework
[38] The Common Criteria, https://www.iso.org/standard/56639.html
[39] ISO38505-1 Data Governance, https://www.iso.org/standard/56639.html

While ISO/IEC 38505-1:2017 looks at the governance of data and its use within an organization, guidance on the implementation arrangement for the effective governance of IT in general is found in ISO/IEC/TS 38501. The constructs in ISO/IEC/TS 38501 can help to identify internal and external factors relating to the governance of IT and help to define beneficial outcomes and identify evidence of success.

ISO/IEC 38505-1:2017 applies to the governance of the current and future use of data that is created, collected, stored or controlled by IT systems, and impacts the management processes and decisions relating to data.

ISO/IEC 38505-1:2017 defines the governance of data as a subset or domain of the governance of IT, which itself is a subset or domain of organizational, or in the case of a corporation, corporate governance.

ISO/IEC 38505-1:2017 is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. This document is applicable to organizations of all sizes from the smallest to the largest, regardless of the extent of their dependence on data.

6.5 Key Standards of System management and organizational governance

The ISO/IEC 27000 series was developed and released by the International Organization for Standardization (ISO) to guide organizations in establishing an information security management system (ISMS). The ISO/IEC 27000 series is a set of internationally accepted and widely used ISMS certification standards. For example, ISO/IEC 27001 sets out requirements that define how to establish, implement, maintain, and continually improve an ISMS. Centering on risk management, ISO/IEC 27001 requires organizations to regularly assess risks and relevant controls to effectively ensure continuous operations of their ISMS. Multiple cloud security standards in the industry are based on the ISO/IEC 27001 ISMS, including CSA Cloud Controls Matrix (CCM), Multi-Tier Cloud Security (MTCS), and Cloud Computing Compliance Criteria Catalogue (C5). In 2019, after incorporating privacy protection control requirements set out in the EU GDPR, the ISMS was extended to the privacy information management system (PIMS), defined in ISO/IEC 27701.

In cloud service environments, organizations can adapt the ISMS to the specific requirements of cloud computing security by implementing ISO/IEC 27017 extended cloud security requirements and ISO/IEC 27018 cloud-specific privacy protection requirements, both of which are based on ISO/IEC 27001.

» **ISO/IEC 27001:2022**[40] specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

  Several cloud security standards are based on the ISO/IEC 27001 ISMS system. In the cloud service environment, organizations can implement the cloud security extension requirements ISO/IEC 27017 and cloud privacy protection requirements ISO/IEC 27018 based on ISO/IEC 27001 to better adapt the information security protection system to the special requirements of cloud computing security.

  ISO/IEC 27001 is a management system standard in the information security field. It proposes 35 control objectives and 114 control measures under 14 control domains for the information security management system, focuses on the construction and implementation of the information security management system, and specifies the basic requirements for organizations to build an information security management system framework. The methods and requirements of information security risk assessment are put forward in the standard category, and the description and content of risk disposal after risk assessment are attached.

» **ISO 27002:2022**[41] provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:
  a) within the context of an information security management system (ISMS) based on ISO/IEC27001;
  b) for implementing information security controls based on internationally recognized best practices;
  c) for developing organization-specific information security management guidelines.

[40] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection- Information security management systems-Requirements, https://www.iso.org/standard/82875.html
[41] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, https://www.iso.org/standard/75652.html

» **ISO/IEC 27011:2016**[42] is to define guidelines supporting the implementation of information security controls in telecommunications organizations.
The adoption of this Recommendation | ISO/IEC 27011:2016 will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.

» **ISO/IEC 27005:2018**[43] provides guidelines for information security risk management. ISO/IEC 27005:2018 supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this standard.

ISO/IEC 27005:2018 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.

» **ISO/IEC 27014:2020**[44] provides guidance on concepts, objectives and processes for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security-related processes within the organization.
The intended audience for this document is:
- governing body and top management;
- those who are responsible for evaluating, directing and monitoring an information security management system (ISMS) based on ISO/IEC 27001;
- those responsible for information security management that takes place outside the scope of an ISMS based on ISO/IEC 27001, but within the scope of governance.

ISO/IEC 27014:2020 is applicable to all types and sizes of organizations. All references to an ISMS in this standard apply to an ISMS based on ISO/IEC 27001.

» **ISO/IEC 27015:2012** provides information security guidance complementing and in addition to information security controls defined in ISO/IEC 27002:2005 for initiating, implementing, maintaining, and improving information security within organizations providing financial services.

» **COBIT**[45] : Information Security serves to extend the COBIT portfolio by building upon best practices shared for the governance and management of information and technology aimed at the whole enterprise through the lens of information security, and details additional metrics and activities that should be considered when implementing or assessing COBIT in the context of information security.

The major drivers for the development of this publication include:
- Clarifying the roles of governance and management and showing how they relate to each other
- Providing a clear end-to-end view into distinction within the enterprise and during all process steps between information security governance and information security management practices
- Providing a comprehensive and holistic guidance on information security – not only to processes but to all components in an enterprise, including organization structure, skills, policies, etc.

Stakeholders throughout the enterprise who interact with information security, whether a board director, CISO or business manager will benefit from guidance on:
- Reduced complexity and increased cost-effectiveness due to improved and easier integration and alignment of information security standards, good practices and/or sector-specific guidelines
- Increased stakeholder satisfaction with information security arrangements and outcomes
- Improved integration of information security in the enterprise
- Informed risk decisions and risk awareness
- Improved prevention, detection and recovery
- Reduced (impact and probability of) information security incidents
- Enhanced support for innovation and competitiveness
- Improved management and optimization of costs related to information security
- Better understanding of information security by stakeholders

[42] ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations, https://www.iso.org/standard/64143.html
[43] ISO/IEC 27005:2018 Information technology-Security techniques -Information security risk management, https://www.iso.org/standard/75281.html
[44] ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security, https://www.iso.org/standard/74046.html
[45] COBIT,https://www.isaca.org/resources/cobit

» **ISO/IEC JTC 1/SC 27**[46] is the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas

» **ISO/IEC JTC 1/SC 40**[47]
Standardization of IT Service Management and IT Governance.
Develop standards, tools, frameworks, best practices and related documents for IT Service Management and IT Governance, including areas of IT activity such as audit, digital forensics, governance, risk management, outsourcing, service operations and service maintenance, but excluding subject matter covered under the scope and existing work programs of JTC 1/SC 27 and JTC 1/SC 38.
The work will initially cover:

- Governance of IT, including the development of the ISO/IEC 38500 series standards and related documents.
- Operational aspects of Governance of IT, including ISO/IEC 30121 Information Technology — Governance of digital forensic risk framework, and interfaces with the management of IT as well as the role of governance in the area of business innovation.
- All aspects relating to IT service management, including the development of the ISO/IEC 20000 series standards and related documents.
- All aspects relating to IT-Enabled Services — Business Process Outsourcing, including the development of the ISO/IEC 30105 series standards and related documents.

» **ISO/IEC 38500:2015**[48] provides guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of information technology (IT) within their organizations.

It also provides guidance to those advising, informing, or assisting governing bodies. They include the following:

- executive managers;
- members of groups monitoring the resources within the organization;
- external business or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies;
- internal and external service providers (including consultants);
- auditors.

ISO/IEC 38500:2015 applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT. These processes can be controlled by IT specialists within the organization, external service providers, or business units within the organization.

ISO/IEC 38500:2015 defines the governance of IT as a subset or domain of organizational governance, or in the case of a corporation, corporate governance.

[46] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, https://www.iso.org/committee/45306.html
[47] ISO/IEC JTC 1/SC 40 IT service management and IT governance, https://www.iso.org/committee/5013818.html
[48] ISO/IEC 38500:2015 Information technology — Governance of IT for the organization, https://www.iso.org/standard/62816.html

ISO/IEC 38500:2015 is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. ISO/IEC 38500:2015 is applicable to organizations of all sizes from the smallest to the largest, regardless of the extent of their use of IT.

The purpose of ISO/IEC 38500:20015 is to promote effective, efficient, and acceptable use of IT in all organizations by:

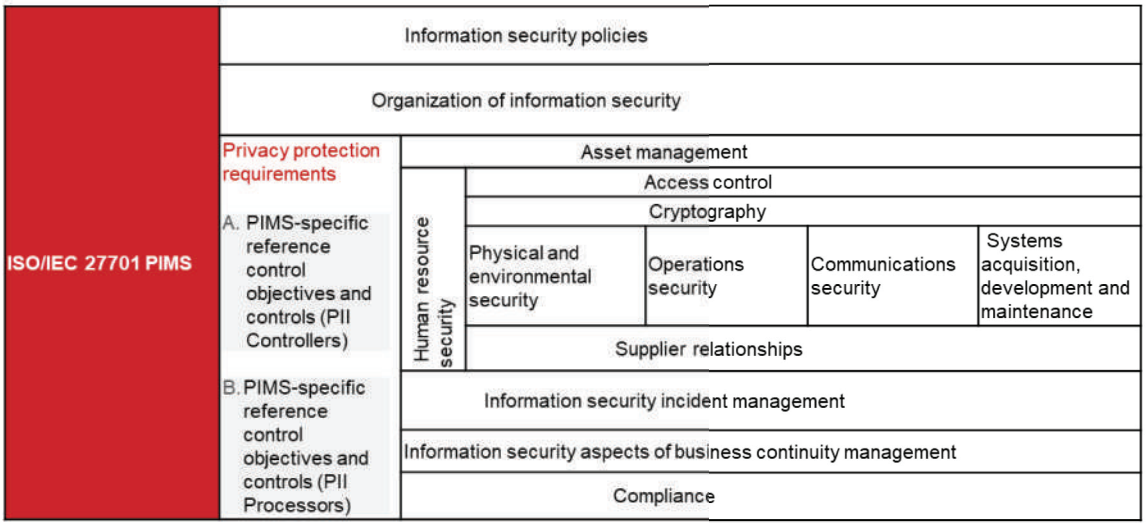
- assuring stakeholders that, if the principles and practices proposed by the standard are followed, they can have confidence in the organization's governance of IT,
- informing and guiding governing bodies in governing the use of IT in their organization, and
- establishing a vocabulary for the governance of IT.

» **ISO/TC309**[49]
Standardization in the field of governance relating to aspects of direction, control and accountability of organizations.

6.6 Key Standards of Personal privacy/information protection

» **ISO/IEC 27701:2019** (PIMS)[50] specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing. ISO/IEC 27701 is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

Figure 8: ISO/IEC 27701 PIMS



» **ISO/IEC 29100:2011**[51] provides a privacy framework which

- specifies a common privacy terminology;
- defines the actors and their roles in processing personally identifiable information (PII);
- describes privacy safeguarding considerations; and
- provides references to known privacy principles for information technology.

ISO/IEC 29100:2011 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.

[49] ISO/TC 309 Governance of organizations, https://www.iso.org/committee/6266703.html
[50] ISO/IEC 27701:2019(en) Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en
[51] ISO/IEC 29100:2011 Information Technology-Security Techniques-Privacy framework, https://www.iso.org/standard/45123.html

» **ISO/IEC 27018:2019**[52] establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

In particular, ISO/IEC 27018:2019 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

ISO/IEC 27018:2019 is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.

ISO/IEC 27018:2019 proposes control requirements on personal privacy data to address the protection of personal identifiable information and privacy principles in cloud services. The 37 control objectives of ISO 27002 extend the PII-related controls and guidance in public cloud services. The standard proposes control requirements on personal privacy data to address the protection of personal identifiable information and privacy principles in cloud services.

» **ISO/IEC 29101:2018**[53] defines a privacy architecture framework that:
- specifies concerns for ICT systems that process PII;
- lists components for the implementation of such systems; and
- provides architectural views contextualizing these components.

ISO/IEC 29101:2018 is applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating ICT systems that process PII.

» **ISO/IEC 29151:2017**[54] establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII).

In particular, this Recommendation | International Standard specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII that may be applicable within the context of an organization's information security risk environment(s).

ISO/IEC 29151:2017 is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities and not-for-profit organizations that process PII.

» **CSA CoC for GDPR Compliance**[55]
The Code of Conduct for GDPR Compliance provides:
Flexibility: Can be applied to any cloud delivery model - IaaS/PaaS/SaaS

Transparency: Provides cloud customers with clear understanding and transparent view of what Cloud Service Provider is doing

Rigor: The CSA CoC provides a rigorous and proven template to adhere to GDPR privacy requirements

Utility: Cloud customers of any size can use this tool to evaluate the level of personal data protection offered by different CSPs (and thus to support informed decisions).

Completeness: Enables CSPs of any size and geographic location with guidance to comply with European Union (EU) personal data protection legislation and to disclose the level of personal data protection they offer to customers.

CoC for Cloud Service Providers:
- Shows adherence to GDPR privacy requirements
- Streamlines contracting, accelerates sales cycles
- Provides assurance to cloud customer of data privacy in conjunction with CSA STAR
- Applies to CSP as Data Processor and as Data Controller
- Demonstrates full compliance by connecting legal to technical

[52] ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, https://www.iso.org/standard/76559.html
[53] ISO/IEC 29101:2018 Information technology-Security techniques-Privacy architecture framework, https://www.iso.org/standard/75293.html
[54] ISO/IEC 29151:2017 Information technology-Security techniques-Code of practice for personally identifiable information protection, https://www.iso.org/standard/62726.html
[55] CSA CoC for GDPR Compliance, https://cloudsecurityalliance.org/privacy/gdpr/code-of-conduct/

CoC for Enterprises:

- Streamlines contracting
- Reduces time needed for internal legal review
- Highlights topics and contracting terms for internal discussion and external negotiation to make informed decisions
- Provides enterprise legal teams with established framework for GDPR compliance when contracting for cloud services

» **NIST Privacy Framework**[56]: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework), to enable better privacy engineering practices that support privacy by design concepts and help organizations protect individuals 'privacy. The Privacy Framework can support organizations in:

- Building customers' trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals 'privacy and society as a whole;
- Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and

Facilitating communication about privacy practices with individuals, business partners, assessors, and regulators.

6.7 Global Advanced Practices

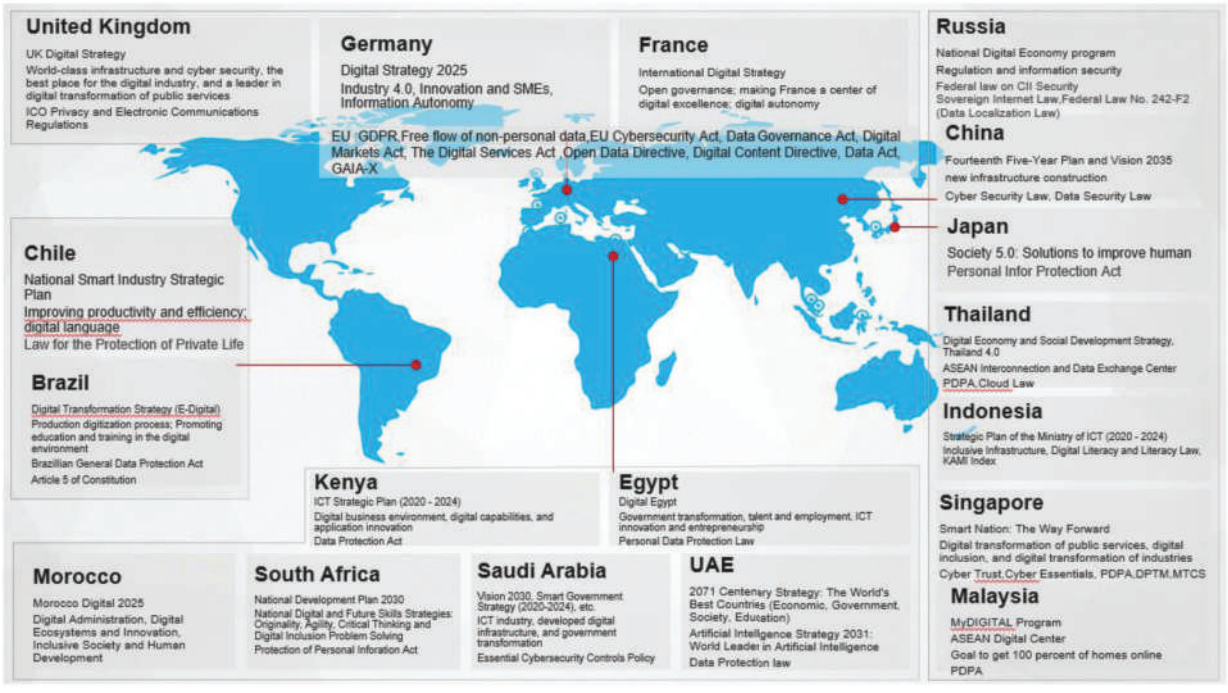
6.7.1 Use case of Data Security Governance at National level

In the digital economy era, data has become a national strategic resource. Data sovereignty = National sovereignty + ICT technology + Global cyberspace + Cross-border data flow in compliance with laws, regulations and standards.

Governments safeguard national sovereignty and data sovereignty by formulating cloud service security and data governance rules and standards to improve national digital economy competitiveness.

More than 170 countries have developed personal privacy/information protection, and data governance's policy, laws, regulations and rules, and are continuously improving and optimizing typical international data security governance standards and cloud service security, such as ISO/IEC standards series, CSA CCM, SOC 1/2/3, NIST CSF, PCI DSS, PCI 3DS and so on.

Figure 9: Landscape of Global Cloud Security and Data Security Legislation and Standardization.



Source: PIKOM Joint Working Group,2022Q4

[56] NIST Privacy Framework, https://www.nist.gov/privacy-framework

» **Europe**

Europe safeguard national sovereignty and data sovereignty through policies and regulations, and promote cloudification, data flow and sharing within the EU, and unlock the value of data with reliable data.

ACT Effective Time / Promulgation Time	Key legislative points for cloud service security and data security governance
GDPR 2018.05. 25 / 2016.04. 14	The GDPR establishes broad and robust privacy and data protection rules. The EU believes that users tend to provide their personal data to controllers they trust, resulting in revenue and economic growth for these organizations, and the GDPR establishes the EU's competitive advantage. Restrictions on cross-border data transfer: In principle, it is prohibited to transfer personal data of EU citizens to countries outside the EU unless the country is deemed by the Commission to provide adequate data protection. Third countries need to ensure that their level of data protection is essentially equivalent to EU safeguards, in particular that effective, independent data protection regulation is in place and that data subjects have effective, enforceable rights and effective administrative and judicial remedies.
NIS Directive 2.0 2024.08/ 2022.05. 05	The NIS Directive of EU puts forward direct requirements for the construction of capability domains such as network and information systems and facility security. Protect the security of critical infrastructure, supply chain, and national security, protect the economic lifeline, and build a resilient, green, and digital Europe.
EU Cybersecurity Act Continuously updated	The EU institutions deal with specific protection measures, technical means, financial and infrastructure construction, public cyber security awareness education, and mutual cooperation between member states. (European Union Agency for Cybersecurity) Support and facilitate the development and implementation of ICT product, ICT service and ICT processing cyber security certification alliance policies.
Free flow of non-personal data 2019.07.16	Note: The EU ensures the free cross-border movement of non-personal data within the EU and prohibits data localization restrictions.
Data Governance Act 2023.09/2022.05	The Data Governance Act was passed in May 2022 and will apply in September 2023. Its purpose is to establish an intermediary structure and enforce the certification of data intermediary service providers. The DGA has clearly defined the data subject (rights). Health and autonomous driving are the two industries most concerned by the EU. It is recommended that public data of the EU be opened to increase trust in data intermediaries and strengthen the data sharing and reuse mechanism across the EU. The EU hopes to capture €700bn of GDP growth through open government data.
Digital Markets Act 2022.07. 19	The aim is to weaken the monopoly of large platforms Gatekeeper, break the control of data by gatekeepers, and promote digital innovation within the EU.
Digital Services Act 2024.01/ 2022.04. 22	Establish a transparency and accountability framework for online platforms and establish organizations for content review. Digital services range from simple websites to Internet infrastructure services and online platforms. Note: Restricting social media "power" and recapturing digital media "right to delete posts" has a huge impact on Internet companies. (Behind the right to delete posts is a huge conflict of legal and value propositions).
Open Data Directive 2019.07. 16	Public sector agencies should make public utility documents and data in a timely manner and bring their formats and metadata into compliance with formal openness standards. Departmental agencies and public utilities shall make their documents available in any existing format or language and, where possible and appropriate, by electronic means, documents and their metadata in a publicly available, machine-readable, accessible, searchable and reusable format. Where possible, formats and metadata should comply with formal open standards.
Data Act 2022.02. 23	The aim is to ensure a better distribution of the value derived from the use of personal and non-personal data among actors in the data economy, particularly with regard to the use of connected objects and the development of the Internet of Things.

Source: PIKOM Joint Working Group,2022Q4

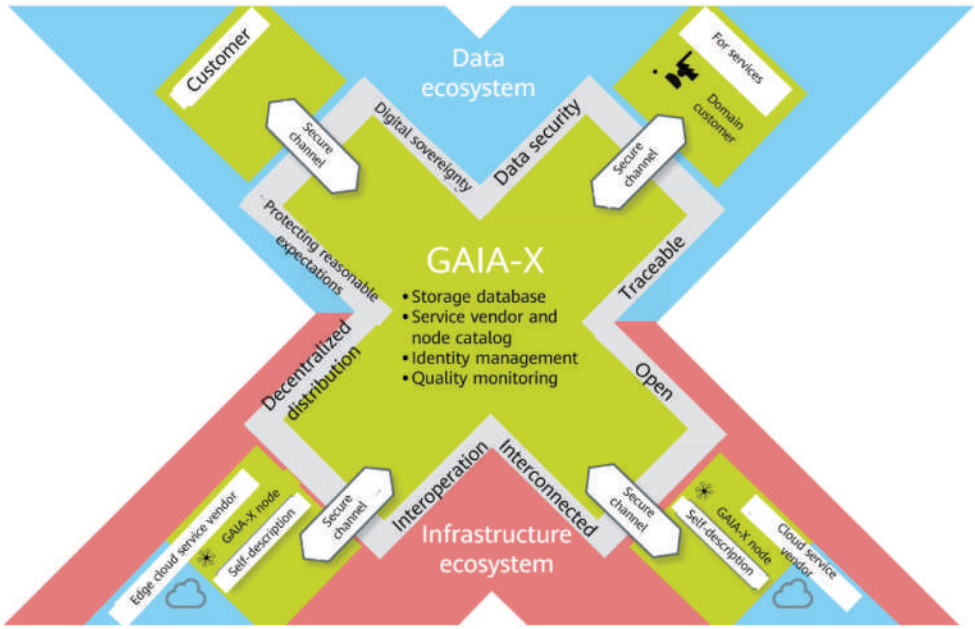
Meanwhile, Europe defend the data sovereignty of European by GAIA-X[57].
GAIA-X is a project reportedly working on the development of a federation of data infrastructure and service providers for Europe with the objective of ensuring a European digital sovereignty. GAIA-X is part of a broader strategy under the von der Leyen Commission of a European strategic autonomy. The project was first presented to the general public at the Digital Summit 2019 in Dortmund (Germany) and has been continuously developed since then. The GAIA-X initiative took the legal form of an AISBL, an in ternational non-profit organization based in Belgium. Initiated by France and Germany, it seeks to create a proposal for the next generation of data infrastructure for Europe, as well as fostering the digital sovereignty of European cloud services users. It is reportedly based on European values of transparency, openness, data protection and security.The name of the project bears reference to the Greek goddess Gaia.

With Gaia-X, representatives from business, science and politics on an international level create a proposal for the next generation of data infrastructure: an open, transparent and secure digital ecosystem, where data and services can be made available, collated and shared in an environment of trust.

Gaia-X is a project initiated by Europe for Europe and beyond. Representatives from business, politics, and science from Europe and around the globe are working together, hand in hand, to create a federated and secure data infrastructure. Companies and citizens will collate and share data – in such a way that they keep control over them. They should decide what happens to their data, where it is stored, and always retain data sovereignty.

The architecture of Gaia-X is based on the principle of decentralization. Gaia-X is the result of a multitude of individual platforms that all follow a common standard – the Gaia-X standard. Together, we are developing a data infrastructure based on the values of openness, transparency, and trust. So, what emerges is not a cloud, but a networked system that links many cloud services providers together.

Figure 10: Gaia-X.



[57] GAIA-X, https://gaia-x.eu/

Global countries are accelerating data residency legislation, with a particular focus on data residence of government data and critical infrastructure data such as transportation, finance, telecommunications, power system and etc..

Country ACT Name Effective Date	Key legislative points for cloud service security and data security governance
Ireland Communications (Retention of Data) Act 2011 2011	A service provider shall retain data in the categories specified in Schedule 2, for a period of 2 years in respect of the data referred to in Part 1 of Schedule 2 (the calling telephone number; the name and address of the subscriber or registered user; the number dialed(the telephone number called) and, in cases involving supplementary services such as call for-warding or call transfer, the number or numbers to which the call is routed; the name and address of the subscriber or registered user; the telephone service used; the calling and called telephone number; the International Mobile Subscriber Identifier (IMSI) of the called and calling parties (mobile telephony only); the International Mobile Equipment Identity (IMEI) of the called and calling parties (mobile telephony only); in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated (mobile telephony only))and for a period of one year in respect of the data referred to in Part 2 of Schedule 2(the user ID allocated; the user ID and telephone number allocated to any communication entering the public telephone network; the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication; the user ID or telephone number of the intended recipient of an Internet telephony call; the name and address of the subscriber or registered user and user ID of the intended recipient of the communication; the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user; the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone; the calling telephone number for dial-up access; the digital subscriber line (DSL) or other end point of the originator of the communication). (2) The periods of retention referred to in subsection (1) commence - (a) in the case of data that before the passing of this Act were the subject of a data retention request under Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, on the date before the passing of this Act on which the data were first processed by the service provider, (b) in any other case, on the date on or after the passing of this Act on which the data were first so processed. (3) Data retained in accordance with subsection (1) shall be retained in such a way that they may be disclosed without undue delay pursuant to a disclosure request. (4) The data referred to in subsection (1) include data relating to unsuccessful call attempts that, in the case of data specified in Part 1 of Schedule 2, are stored in the State, or in the case of data specified in Part 2 of Schedule 2, are logged in the State. (5) This section does not require a service provider to retain aggregated data, data that have been made anonymous or data relating to unconnected calls. (6) In this section "aggregated data" means data that cannot be related to individual subscribers or users. Note: Carrier operators' data storage require within territory to prevent accidental or unlawful destruction, accidental loss or alteration, unauthorized or illegal storage, processing, access or disclosure of data; Ensure that only authorized personnel have access to the data; Implement data destruction measures.
Kazakhstan Law On Communications amended on 2022.07.14/2004.07.05	Communication operators and (or) owners of communication networks operating on the territory of the Republic of Kazakhstan shall be obliged to: 1) provide the bodies carrying out operational-investigative, counterintelligence activities on communication networks with organizational and technical capabilities of conducting operational-investigative, counterintelligence actions on all communication networks, as well as take measures for prevention of disclosure of forms and methods for conducting the specified actions; 2) collect and store official information in the manner determined by the Government of the Republic of Kazakhstan. Storage of official information about the subscribers shall be carried out exclusively on the territory of the Republic of Kazakhstan. It is forbidden to transfer official information about the subscribers outside the Republic of Kazakhstan, except for the cases of provision of communication services to the subscribers of the Republic of Kazakhstan located abroad. Note: The data about subscribers of communications services are stored only in Kazakhstan, and it is prohibited to transfer them abroad, except for the scenario where services are provided to citizens of Kazakhstan abroad.
Nigeria Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) Cybercrimes Act 2022.06. 30	2. Host all sovereign data (sovereign data hosted by ministries, departments, and agencies of Nigeria's government federal and information management companies) locally within the country and shall not for any reason host any sovereign data outside the country without an express approval from NITDA. Note: Localized storage of government data: Government data should be stored in Nigeria. If the data needs to be transferred to other countries, it should be approved by NITDA in advance. Local storage of traffic data and subscriber information for at least two years.
Saudi Arabia Cloud Computing Regulatory Framework 2019.06. 13	3.3.9 Cloud Customers may not transfer, store or process Level 3 Customer Content to or in any Public Cloud, Community Cloud or a Hybrid Cloud, unless and for as long as the CSP is validly registered with the Commission pursuant to article 3.2, above. Note: Level-3 customer content must be stored locally and cannot be transferred outside territory.

UAE Regulatory Framework for Stored Values and Electronic Payment Systems 2020.12. 10	D.6.1PSPs (digital payment service provider, any institution licencedor authorized to provide digital payment services, including Retail PSP, Micropayments PSP, Government PSP, and Non-issuing PSP) must store and retain all User and transaction data exclusively within the borders of the UAE, (excluding UAE financial Free Zones), for a period of five (5) years from the date of the original transaction. Note: Digital payment service providers should pay attention to their requirements for localized storage of transaction data.
South Korea Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc Act on The Establishment, Management, Etc. of Spatial Data Amended by Act No. 13520, Dec. 1, 2015	Article 51: (1) The Government may have providers or users of information and communications services to take necessary measures to prevent outflow abroad of any important information about industry, economy, science, technology, etc. of this country through information and communications networks. (2) The scope of the important information under paragraph (1) shall be as follows: 1. Information related to the national security and major policies; 2. Information about details of cutting-edge science and technology or equipment developed within this country. Note: • For communications services customers, they should be assisted in localizing the storage of any important information relating to industry, economics, science and technology, as well as information relating to national security and major policies, as well as detailed information on cutting-edge science, technology or equipment developed in their own countries. • Maps, etc., or photographs for survey purposes obtained in basic surveys/public surveys shall not be taken out of the country without the permission of the Minister of Land, Infrastructure and Transport.
Singapore Singapore Cybersecurity Ordinance (CYBERSECURITY ACT 2018) Singapore Personal Data Protection Act (PERSONAL DATA PROTECTION ACT 2012) 2021.01. 22	Focus on the National Basic Information Infrastructure (Critical Information Infrastructure), covering 11 industries: Aviation, Banking & Finance, Energy, Government, Healthcare, Infocomm, Land Transport, Maritime, Media, Security & Emergency Services and Water. Personal Data: Organizations cannot transfer mission personal data out of the country unless the organization provides the same standard of protection as the statute provides. Singapore took the lead in developing the ASEAN Data Management Framework (DMF) and ASEAN Model Contracts for Cross-border Data Flows (MCCs) to promote the development of the digital economy. The Singapore PDPC 2021.01.22 published "A Guide to the Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows in Singapore", which lists four key clarifications and amendments on how the ASEAN MCC can be adapted to the Singapore PDPA.
Philippines Department_Circular_No_10_Amendments_to_DC_No_2017_002_re_Prescribing 2022.06	In June 2020, DICT issued a document No. 2020 - 010 amending the above-mentioned cloud priority policy, including the scope of the cloud priority policy, government data classification, government data security requirements, and government data sovereignty and ownership, to strengthen the Philippine government's control over government data. Note: Government data is stored locally.
Indonesia Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82) 2012	Article 17 (2) Electronic System Operator for the public service is obligated to put the data center and disaster recovery center in Indonesia for the purpose of law enforcement, protection, and enforcement of national sovereignty to the data of its citizens. (Electronic System Operator is any Person, state agency, Business Entity, and community that provide, manage, and/or operate Electronic System individually or jointly to Electronic System User for its interest or other party's interest.) (3) Further provisions on the obligation of placing the data center and disaster recovery center in Indonesian territory as intended in paragraph (2) shall be governed by related Sector Supervisory and Regulatory Agency in accordance with the provisions of regulation after coordination with the Minister. Article 43 The Electronic Transactions (Electronic Transaction is a legal act that is conducted by the use of Computers, Computer networks, and/or other electronic media)in the territory of the Republic of Indonesia shall: perform transactions data storage in domestically Note: The data center and disaster recovery center are located in Indonesia. Electronic transaction data is stored in Indonesia.
Indonesia Government Regulation No. 71 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82) 2019	Indonesia has issued a government regulation in the scope of information and electronic transactions namely Government Regulation No. 71 of 2019 on Organization of Electronic Systems and Transactions (GR 71/2019). This regulation comes to substitute for the previous regulation, Government Regulation Number 82 of 2012 on Organization of Electronic Systems and Transactions (GR 82/2012). In its transitional provision, the Private ESP that has been in operation before the promulgation of GR 71/2019, must adjust to the provisions in Article 6 (regarding registration obligation) within 1 year. The GR 71/2019 became effective on 10 October 2019, so the deadline for Private ESP to adjust is until 10 October 2020.

	Note: Data Center Placement Concern over the obscurity of Data Center placement on GR 82/2012 has now been given legal certainty, that is: For the Public ESP is required to manage, process, and/or store Electronic Systems and Electronic Data in the territory of the Republic of Indonesia, but it is excluded if it is not yet available. Private ESP can manage, process, and/or store Electronic Systems and Electronic Data in the Republic of Indonesia and/or outside Indonesia. If management is carried out outside, it must ensure the effectiveness of supervision by the ministry, etc. The financial sector will be regulated further by BI and OJK.
Bangladesh DATA PROTECTION ACT 2022 Request for Comments	The sensitive data, user created or generated data and classified data shall be stored in Bangladesh, and shall remain beyond the jurisdiction of any court and law enforcers other than Bangladesh.

Source: PIKOM Joint Working group, 2022Q4

» **Korea K-ISMS**[58] **:**

Under Article 47 in the "Act on Promotion of Information and Communications Network Utilization and Information Protection", the Korean government introduced the Korea-Information Security Management System (K-ISMS). A country-specific ISMS framework, it defines a stringent set of control requirements designed to help ensure that organizations in Korea consistently and securely protect their information assets.

To obtain the certification, a company must undergo an assessment by an independent auditor that covers both information security management and security countermeasures. It covers 104 criteria including 12 control items in 5 sectors for information security management, and 92 control items in 13 sectors for information security countermeasures. Some of these criteria include examination of the organization's security management responsibilities, security policies, security training, incident response, risk management, and more. A special committee examines the results of the audit and grants the certification.

The K-ISMS framework is built on successful information security strategies and policies. It also accounts for security countermeasures and threat response procedures to minimize the impact of security breaches. These procedures have a significant overlap with ISO/IEC 27001 control objectives but are not identical. K-ISMS provides a more detailed investigation against requirements than a general ISO/IEC 27001 assessment.

Under the supervision of the Korean Ministry of Science and Information Technology (MSIT), the Korea Internet & Security Agency (KISA) is the K-ISMS certifying authority. Certification is valid for three years, and certified entities must pass an annual audit to maintain it.

» **Singapore MTCS**[59] **:**

MTCS was prepared under the direction of the Information Technology Standards Committee (ITSC) of the Infocomm Media Development Authority (IMDA). It is the first cloud security standard with different levels of security, so certified CSPs can specify which levels they offer.

MTCS builds upon recognized international standards, such as ISO/IEC 27001, and covers such areas as data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery, and incident management.

MTCS aims to provide:

- A common standard that CSPs can apply to address customer concerns about the security and confidentiality of data in the cloud, and the impact on businesses of using cloud services;
- Verifiable operational transparency and insight into risks to customers when they use cloud services.

The MTCS covers 19 domains of six categories: cloud governance, cloud infrastructure security, cloud operation management, cloud service management, cloud user access rights, and tenant isolation. The MTCS has three levels (level-1 to level-3) to authenticate cloud service providers based on different levels of requirements. The level-3 is the most demanding and safest. Cloud service providers must have strict security plans and undergo annual audits by MTCS certification bodies before they can pass MTCS level-3 certification.

It also includes a mechanism for customers to benchmark and rank the capabilities of CSPs against a set of minimum baseline security requirements.

[58] Korea K-ISMS, https://isms.kisa.or.kr/main/isms/intro/
[59] Singapore MTCS, https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Media-Releases/2013/new-multi-tier-cloud-security-mtcs-standard-launched-in-singapore

» **Germany C5[60] :**

C5 is a German Government-backed attestation scheme introduced in Germany by the Federal Office for Information Security (BSI) to help CSPs demonstrate operational security against common cyber-attacks when using cloud services within the context of the German Government's "Security Recommendations for Cloud Providers".

Cloud computing is based on a high degree of standardization of hardware and software, as well as the services based on it, the details of which are usually not known to the customers. As a result, CSPs must establish and maintain a particularly high level of trust.

The purpose of C5 is to assess the information security of cloud services in order to establish trust. Established standards for information security (e.g., ISO/IEC 27001 and CSA CCM) formed the basis for the criteria and made it possible for auditors to carry out audits in accordance with international audit standards.

This criteria catalogue contains 17 objectives regarding the information security of cloud services. Each objective is broken down into the criteria required to achieve the objective. The criteria are divided into basic criteria and additional criteria.

Figure 11: Germany C5:2020 Cloud security management framework

The basic criteria reflect the minimum level of information security that a CSP must offer when CSCs use cloud services. The basic criteria define the minimum scope of an audit according to C5. For CSCs whose information has a higher need for protection, the additional criteria provide a starting point for conducting this assessment. CSPs may include other security criteria when performing as sessment according to C5.

CSCs stay informed about the security controls implemented by CSPs to meet C5 requirements on the basis of information in the C5 attestation report, and assess the suitability of the design and operating effectiveness of the control mechanism.

Establishing such security frameworks makes it easier for organizations to understand the security measures they need to implement and the expertise they need to do so. However, these frameworks are not associated with cloud service management processes, and therefore it is difficult for functional departments to understand the security responsibilities within their roles. As a result, some security responsibilities may be left unassigned.

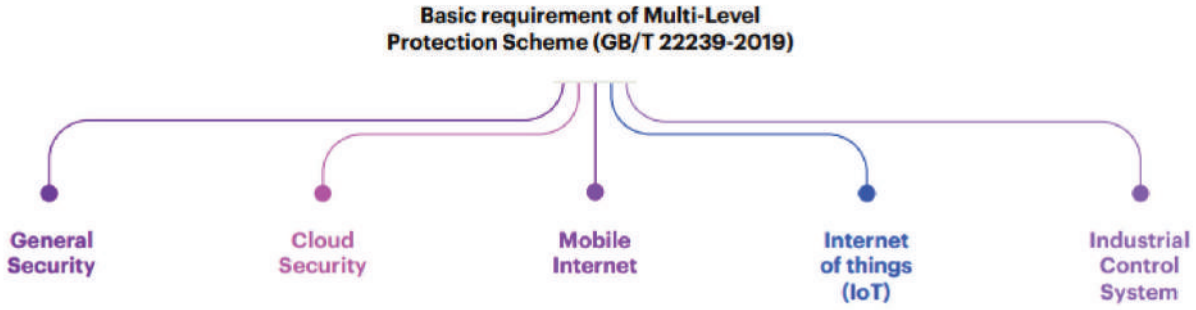
[60] Germany C5, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

» **China GB/T 22239-2019**[61]

CSL Article 21(Cybersecurity Law (Effective in June 2017)): The State has implemented a cybersecurity MLPS. Network operators must perform the following security protection duties according to the requirements of the cybersecurity MLPS to ensure the network is free from interference, damage, or unauthorized access, and to prevent network data leaks, theft, or falsification…

GB/T 22239-2019 Information security technology-Baseline for classified protection of cybersecurity. GB/T 22239-2019 specifies the general security requirements and security extension requirements for the project under classified protection from level 1 to level 4 of the classified protection of cybersecurity.

Figure 12: GB/T 22239-2019



Network Operators are obliged to comply with the general security requirements which must be met regardless of the form of the level of protection. Other special requirements for Cloud, Mobile Internet, Internet of Things, and Industrial Control Systems,which are called security expansion requirements.

More details as:
https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=BAFB47E8874764186BDB7865E8344DAF

» **China GB/T 31168-2014**[62]

Information security technology—Security capability requirements of cloud computing services (GB/T 31168-2014) is a cloud computing service security standard issued by the China Information Security Standardization Technical Committee (SAC/TC260). It is oriented to cloud service providers and sets out the security capability requirements that cloud service providers should have when providing services to government departments. This standard is applicable to cloud service providers that provide cloud computing services for governments. Based on the sensitivity and importance of information on the cloud computing platform, the standard is classified into general requirements and enhanced requirements. The required capabilities are also different.

This standard focuses on service availability and security, differentiates responsibilities based on service types, and proposes 10 types of security requirements: System development and supply chain security, system and communication protection, access control, configuration management, mainte nance, emergency response and disaster recovery, audit, risk assessment and continuous monitoring, security organization and personnel, and physical and environmental protection.

[61] China GB/T 22239-2019, https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=BAFB47E8874764186BDB7865E8344DAF
[62] China GB/T 31168-2014, https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=6630D5BE60B49E0414EB951BC354618B

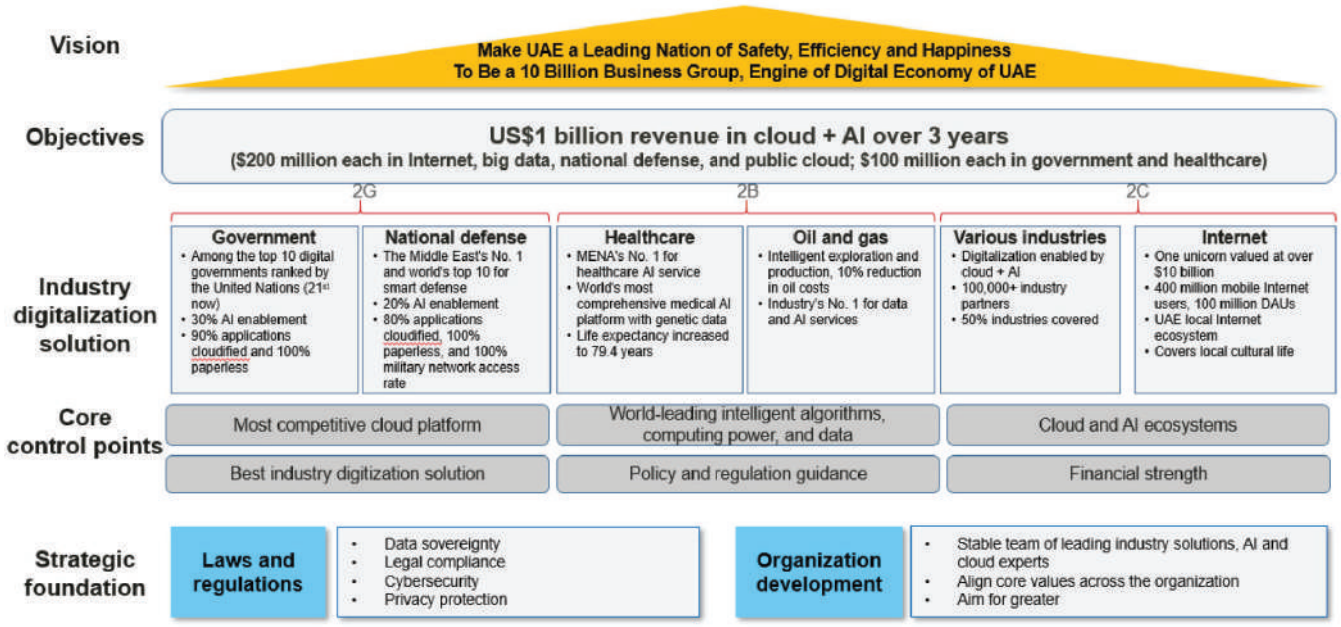
» **UAE G42[63] Strategy: Build Most Competitive Cloud + AI Infra, Enable Digital Economy of UAE Government-led Cloud Construction and a Target-driven Approach to the Engine of Digital Economy**

Group 42 (also known as G42) is an artificial intelligence and cloud computing company that was founded in Abu Dhabi, United Arab Emirates (UAE) in 2018. The organization is oriented to development of AI industries in the government sector, healthcare, finance, oil and gas, aviation and hospitality. G42 develops and deploys high-impact industry solutions in sectors like the government, healthcare, finance, sports, energy and smart cities.

In addition to conducting research and delivering industry solutions that address near term opportunities, Group 42 is also working towards a future where AI will be able to handle generalized tasks, much like humans do, in what will be the age of Artificial General Intelligence.

G42 has an active and extensive partnership network, connecting leading international organizations who complement its ecosystem and supports its vision. G42 partnerships range from strategic teaming agreement, joint ventures, to direct investments by the Group.

Figure 13: G42 Vision and Mission



6.7.2 Use Case of Data Security Governance in vertical Industries

» **Key Standards in Financial**

PCI DSS[64]

The Payment Card Industry (PCI) Data Security Standards (DSS) is a global information security standard designed to prevent fraud through increased control of credit card data. The PCI Security Standards Council (PCI SSC) is a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards, including PCI DSS.

Compliance with PCI DSS is required for any organization that stores, processes, or transmits cardholder data, which, at a minimum, consists of the full primary account number (PAN) – a unique payment card number that identifies the issuer and the particular cardholder account. Cardholder data may also appear in the form of a full PAN plus additional information such as cardholder name, expiration date, and service codes. Sensitive authentication data that may be transmitted or processed (but not stored) as part of a payment transaction contains additional data elements that must also be protected, including track data from card chip or magnetic stripe, PINs, PIN blocks, and so on. For more information, see PCI DSS glossary.

[63] UAE G42, https://www.mubadala.com/en/what-we-do/g42
[64] PCI DSS, https://www.pcisecuritystandards.org/document_library/

The PCI DSS designates four levels of compliance based on transaction volume, with Service Provider Level 1 corresponding to the highest volume of transactions at more than 6 million a year. The assessment results in an Attestation of Compliance (AoC), which is available to customers and Report on Compliance (RoC) issued by an approved Qualified Security Assessor (QSA). The effective period for compliance begins upon passing the audit and receiving the AoC from the QSA and ends one year from the date the AoC is signed.

OSPAR (Singapore)[65]

The Association of Banks in Singapore (ABS) has issued the ABS Guidelines on Control Objectives and Procedures for Outsourced Service Providers (ABS Guidelines). The ABS Guidelines contain information security guidance for service providers who deliver services to financial institutions operating in Singapore. The guidelines specify the baseline organizational controls that service providers must implement in cloud outsourcing arrangements, particularly for workloads with material impact. The Outsourced Service Provider's Audit Report (OSPAR) is the framework that external auditors use to validate the service provider's controls against the criteria specified in the ABS Guidelines.

PCI 3DS[66]

Europay, Mastercard, and Visa (EMV) three-domain secure (3-D Secure or 3DS) is an EMVCo messaging protocol that enables cardholders to authenticate with their card issuers when making card-not-present (CNP) online transactions. The specification aims at securing authentication and identity verification in mobile and browser-based applications. The additional security layer helps prevent unauthorized CNP transactions and protects the merchant from exposure to CNP fraud.

The three domains in the EMVCo specification include:
Acquirer domain: 3DS transactions are initiated from the acquirer domain. The components under this domain are the 3DS Server (3DSS), requester environment, integrator, and acquirer.

Interoperability domain: Facilitates the transfer of transaction information between the acquirer domain and issuer domain. The components under this domain are the 3DS Directory Server (DS), Directory Server Certificate Authority (DS-CA), and authorization system.

Issuer domain: 3DS transactions are authenticated in the issuer domain. The components under this domain are the 3DS Access Control Server (ACS), cardholder, consumer device, and issuer.

The three critical EMV 3DS components or functions across these domains include:
3DS Server (3DSS), 3DS Directory Server (DS), 3DS Access Control Server (ACS).

The PCI 3DS Core Security Standard provides a framework for these critical EMV 3DS functions to implement security controls that support the integrity and confidentiality of 3DS transactions. The standard applies to entities that perform or provide these functions (3DSS, DS, and ACS), as defined in the EMVCo 3DS Core Specification. Third-party service providers that can impact these 3DS functions, or the security of the environments where these functions are performed, may also be required to meet PCI 3DS requirements. Whether an entity is required to validate compliance with the PCI 3DS Core Security Standard is defined by the individual payment brand compliance programs.

» Key Standards in Carrier

The Global System for Mobile Communications Association (GSMA) is an industry organization that "represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors." The GSMA established the Security Accreditation Scheme (SAS) to enable mobile operators to assess the security of their Universal Integrated Circuit Card (UICC)[67] and embedded UICC (eUICC) suppliers, as well as their eUICC subscription management service providers. Two schemes operate under SAS:
SAS for UICC Production (SAS-UP) is a well-established scheme through which UICC and eUICC manufacturers subject their production sites and processes to a comprehensive security audit. SAS for Subscription Management (SAS-SM) is a related security auditing and accreditation scheme

[65] OSPAR(Singapore), https://www.abs.org.sg/industry-guidelines/outsourcing
[66] PCI 3DS, https://www.emvco.com/emv-technologies/3d-secure/
[67] UICC and eUICC, https://www.gsma.com/security/security-accreditation-scheme/

for the providers of eUICC subscription management services, intended to ensure industry confidence in the security of remote provisioning for eUICCs.

The GSMA's established Security Accreditation Scheme (SAS) is the required security accreditation for embedded subscriber identity module (eSIM) entities handling sensitive assets, including mobile network operator (MNO) profile information and digital certificates. SAS-SM audits the robustness of processes for secure data management at the subscription management service location.

» Key Rules in Healthcare and life sciences

USA HIPAA[68] : The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations issued under HIPAA are a set of US healthcare laws that, among other provisions, establish requirements for the use, disclosure, and safeguarding of protected health information (PHI). The scope of HIPAA was extended in 2009 with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act that was created to stimulate the adoption of electronic health records and supporting information technology.

HIPAA applies to covered entities-doctors'offices, hospitals, health insurers, and other healthcare companies-that create, receive, maintain, transmit, or access PHI. HIPAA further applies to business associates of covered entities that perform certain functions or activities involving PHI as part of providing services to the covered entity or on behalf of the covered entity. When a covered entity engages the services of a cloud service provider (CSP), such as Microsoft, the CSP becomes a business associate under HIPAA. Moreover, when a business associate subcontracts with a CSP to create, receive, maintain, or transmit PHI, the CSP also becomes a business associate.

Together, HIPAA and HITECH Act rules include:
The Privacy Rule, which requires appropriate safeguards to protect the privacy of PHI and imposes restrictions on the use and disclosure of PHI without patient authorization. It also gives patients the rights over their health information, including rights to examine their health records and request corrections.

- The Security Rule, which sets the standards for administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.
- The Breach Notification Rule, which requires covered entities and their business associates to provide notification when a breach of unsecured PHI occurs.

HIPAA regulations require that covered entities and their business associates enter into a contract called a Business Associate Agreement (BAA) to ensure the business associates protect PHI adequately. Among other things, a BAA establishes the permitted and required uses and disclosures of PHI by the business associate, based on the relationship between the parties and the activities and services being performed by the business associate.

» Key Standards in Media

The Content Delivery & Security Association (CDSA)[69] is a worldwide forum advocating for the innovative and responsible delivery and storage of entertainment, software, and information content. CDSA provides community, collaboration, and communications services that protect entertainment media throughout the supply chain. In 2018, CDSA and the Motion Picture Association (MPA) launched the Trusted Partner Network (TPN) to help the industry improve content security, simplify assessments, and enable content owners to gauge their level of conformance to the MPA content protection best practices.

The CDSA Content Protection & Security (CPS) Standard provides guidance and requirements for securing media assets within a Content Security Management System (CSMS). The standard specifies a set of controls designed to ensure the integrity of intellectual property and the confidentiality and security of media assets at every stage of the digital media supply chain.

The CPS certification audit used to be administered directly by the CDSA. It consists of over 300 distinct controls that help secure and manage physical data centers, harden services, and protect storage facilities. All controls are optimized to handle sensitive and valuable media assets. Once a system was validated by the CDSA assessor, the CDSA would issue a certificate of compliance. To

[68] USA HIPAA, https://www.cdc.gov/phlp/publications/topic/hipaa.html
[69] CPS certification audit, https://www.cdsaonline.org/cps-standard/

maintain compliance, the certified entity was required to submit the results of annual audits to the CDSA.

Since launching the TPN, both the MPA and CDSA have ceased their individual security assessment programs to focus on managing and developing the TPN program and TPN annual assessments. Past audits or assessments will remain valid for the period originally indicated but will not be renewable within their individual programs. For both the MPA and CDSA, the primary focus is to provide a unified assessment program through the TPN.

» **Key Standards in Automotive**

The Trusted Information Security Assessment Exchange (TISAX)[70] is administered by the ENX Association on behalf of the German Association of the Automotive Industry (Verband der Automobilindustrie, VDA).

VDA developed an information security assessment (ISA) as a catalog of criteria for assessing information security. The VDA ISA is based on the ISO/IEC 27001 and ISO/IEC 27002 standards adapted to the automotive industry. In 2017, the VDA assessment was updated to cover controls for the use of cloud services.

VDA member companies used the ISA both for internal security assessments and for assessments of suppliers, service providers, and other partners that process sensitive information on their behalf. However, because these evaluations were handled individually by each company, they created a burden on partners and duplicated efforts on the part of VDA members.

To help streamline security evaluations, VDA set up TISAX, which is used by European automotive companies to provide a common information security assessment for internal analysis, evaluation of suppliers, and information exchange. The ENX Association is responsible for TISAX implementation - it accredits auditors, maintains the accreditation criteria and assessment requirements, and monitors the quality of implementation and assessment results.

The latest TISAX control scope is documented in the VDA ISA catalogue version 5.1

» **Key Standards in Healthcare industry**

ISO 27799:2016[71] gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

It defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard.

ISO 27799:2016 provides implementation guidance for the controls described in ISO/IEC 27002 and supplements them where necessary, so that they can be effectively used for managing health information security. By implementing ISO 27799:2016, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care.

ISO 27799:2016 applies to health information in all its aspects, whatever form the information takes (words and numbers, sound recordings, drawings, video, and medical images), whatever means are used to store it (printing or writing on paper or storage electronically), and whatever means are used to transmit it (by hand, through fax, over computer networks, or by post), as the information is always be appropriately protected.

ISO 27799:2016 and ISO/IEC 27002 taken together define what is required in terms of information security in healthcare, they do not define how these requirements are to be met. That is to say, to the fullest extent possible, ISO 27799:2016 is technology-neutral. Neutrality with respect to implementing technologies is an important feature. Security technology is still undergoing rapid development and the pace of that change is now measured in months rather than years. By contrast, while subject to periodic review, International Standards are expected on the whole to

[70] Trusted Information Security Assessment Exchange (TISAX), https://www.vda.de/vda/en/news/publications/publication/vda-isa-catalogue-version-5.1
[71] ISO 27799:2016 Health informatics-Information security management in health using ISO/IEC 27002, https://www.iso.org/standard/62777.html

remain valid for years. Just as importantly, technological neutrality leaves vendors and service providers free to suggest new or developing technologies that meet the necessary requirements that ISO 27799:2016 describes.

As noted in the introduction, familiarity with ISO/IEC 27002 is indispensable to an understanding of ISO 27799:2016.

The following areas of information security are outside the scope of ISO 27799:2016:

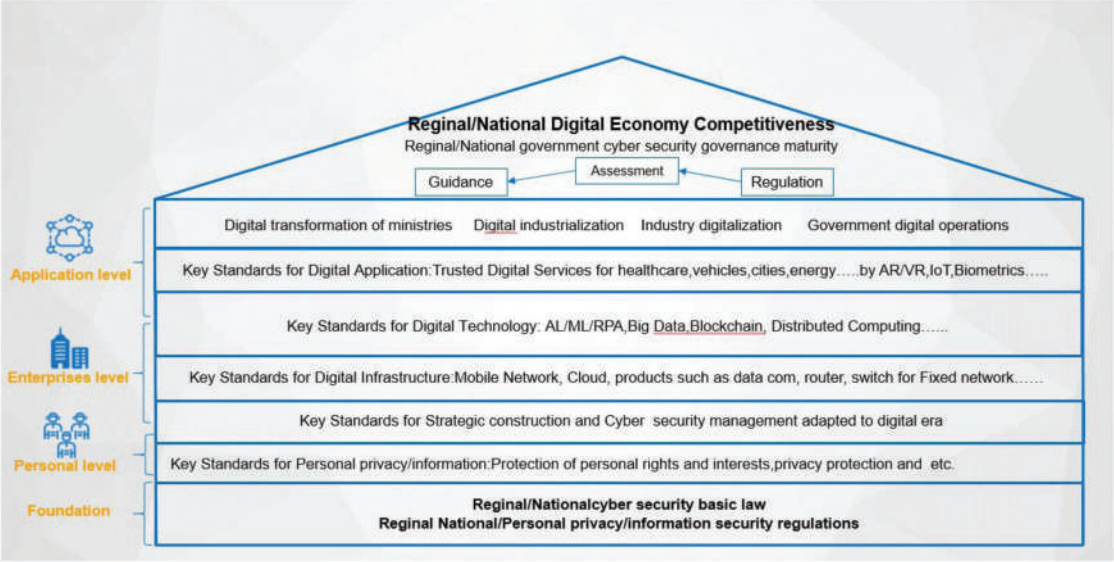
a) methodologies and statistical tests for effective anonymization of personal health information;
b) methodologies for pseudonymization of personal health information (see Bibliography for a brief description of a Technical Specification that deals specifically with this topic);
c) network quality of service and methods for measuring availability of networks used for health informatics;
d) data quality (as distinct from data integrity).

7 RECOMMENDATIONS AND WAY FORWARD

7.1 Digital Trade Standards Systems Framework

ICT is transforming industries and governments around the world, making them digital and intelligent. We call on unleashing the value of reliable data and accelerate digital transformation at the country and enterprise from the perspectives of sovereignty, economic development and cyber security based on Digital Trade Standards Systems Framework.

Figure 14: Digital Trade Standards Systems Framework



This digital trade standards systems could be a reference to facilitate Malaysia to implement international cyber security standards at national level in line with Malaysia's domestic situations.

Meanwhile, to improve national digital economic competitiveness and safeguard national data sovereignty can refer to the following steps:

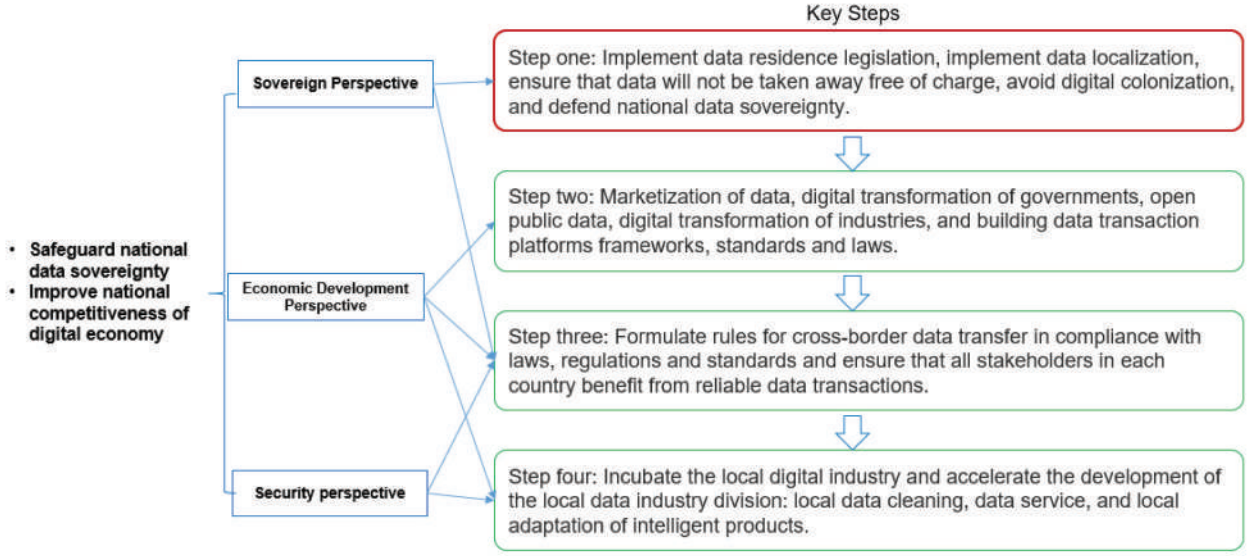
Step 1: Implement data residence t legislation, implement data localization, ensure that data will not be taken away free of charge, avoid digital colonization, and defend national data sovereignty.

Step 2: Marketization of data, digital transformation of governments, open public data, digital transformation of industries, and building data transaction platforms frameworks, standards and laws.

Step 3: Formulate rules for cross-border data transfer in compliance with laws, regulations and standards and ensure that all stakeholders in each country benefit from reliable data transactions.

Step 4: Incubate the local digital industry and accelerate the development of the local data industry division: local data cleaning, data service, and local adaptation of intelligent products.

Figure 15: The perspectives of sovereignty, economic development and cyber security



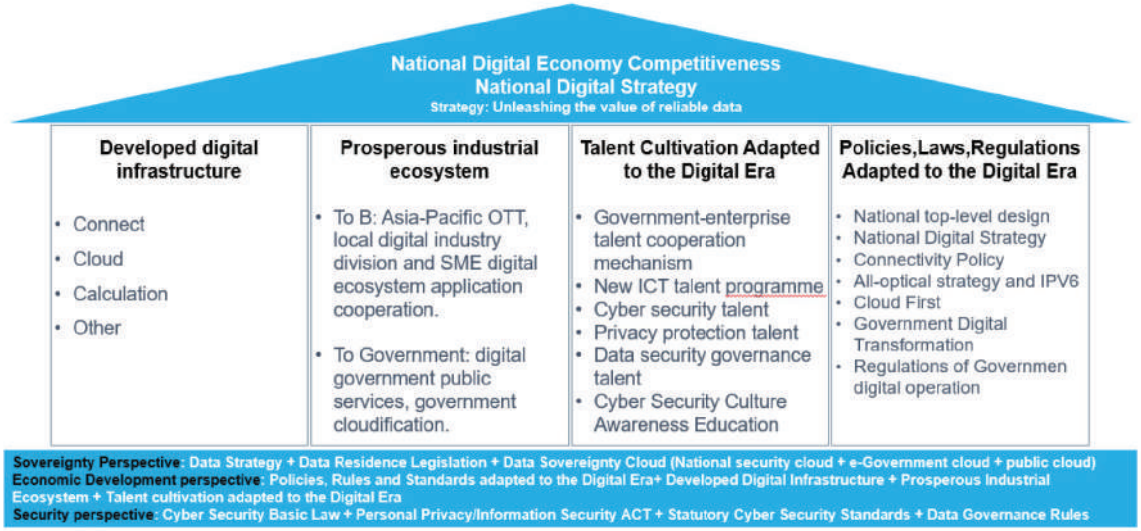
Source: PIKOM Joint Working Group,2022Q4

7.2 Unleashing the value of reliable data

Following is proposed 6 key points regarding on unleashing the value of reliable data:

1. The governments take the lead in formulating national data strategies, legislating on data residence, and defend national data sovereignty.

Figure 16: National Digital Economy Competitiveness



Healthy and Fast Developing Asia-Pacific Digital Economy is including 4 parts:

1. Developed digital infrastructure,
2. Prosperous industrial ecosystem,
3. Talent cultivation adapted to the Digital Era,
4. Policies, Laws, Regulations and Standards adapted to the Digital Era.

The strategy of data security in digital economy and society is unleashing the value of reliable data by:

- **Sovereignty Perspective**: Data Strategy + Data Residence Legislation + Data Sovereignty Cloud (National security cloud + e-Government cloud + public cloud)
- **Economic Development perspective**: Policies, Rules and Standards adapted to the Digital Era+ Developed Digital Infrastructure + Prosperous Industrial Ecosystem + Talent cultivation adapted to the Digital Era.
- **Security perspective**: Cyber Security Basic Law + Personal Privacy/Information Security ACT + Statutory Cyber Security Standards + Data Governance Rules

The ultimate purpose of data security governance is to create value. The government's data security governance maturity is a necessity to improve the competitiveness of a country's digital economy. It is recommended that government data governance legislation can take a great balance between economic development and cyber security.

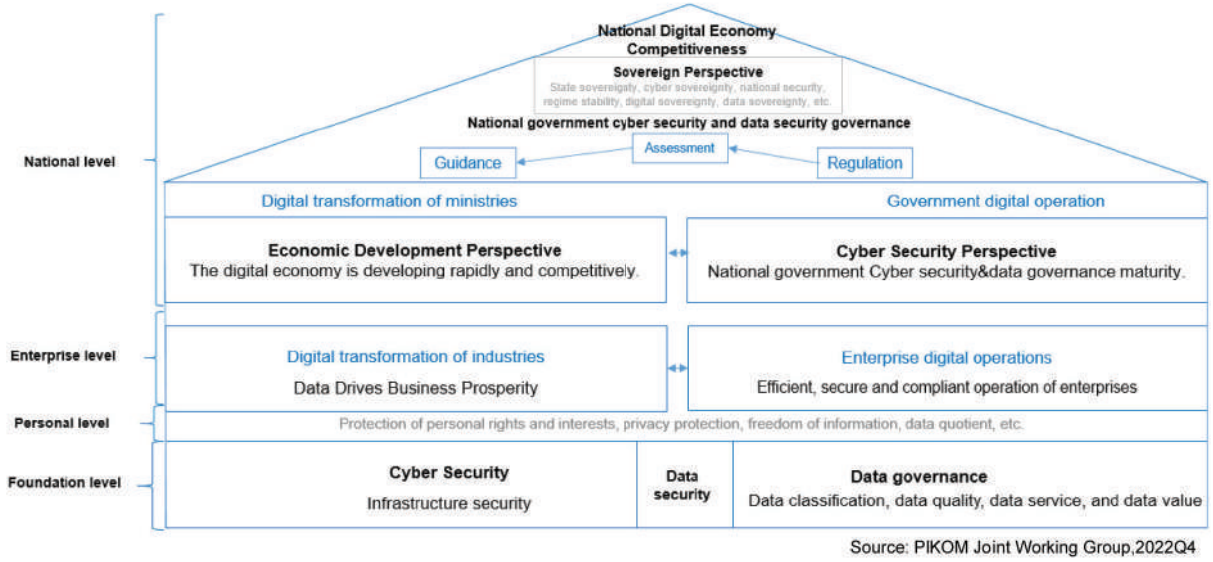
At National level:
From Economic Development Perspective: The national target is the digital economy is developing rapidly, healthy, competitively and collaboratively.
From Cyber Security Perspective: The government's cyber security maturity is a necessity to improve the competitiveness of a country's digital economy.

At Enterprise level:
From Economic Development Perspective: Data Drives Business Prosperity.
From Cyber Security Perspective: Cyber security is an important support for digital operations. Digital transformation of industries needs Efficient, secure and compliant operation of enterprises.

At Personal level:
Protection of personal rights and interests, privacy protection, freedom of information, data quotient and etc shall to be considered.

At Foundation level:
Cyber Security is equal to Infrastructure security, Data governance is equal to Data classification, data quality, data service and data value and data security which is a subset of Cyber Security.

Figure 17: The perspectives of economic development and cyber security



Source: PIKOM Joint Working Group,2022Q4

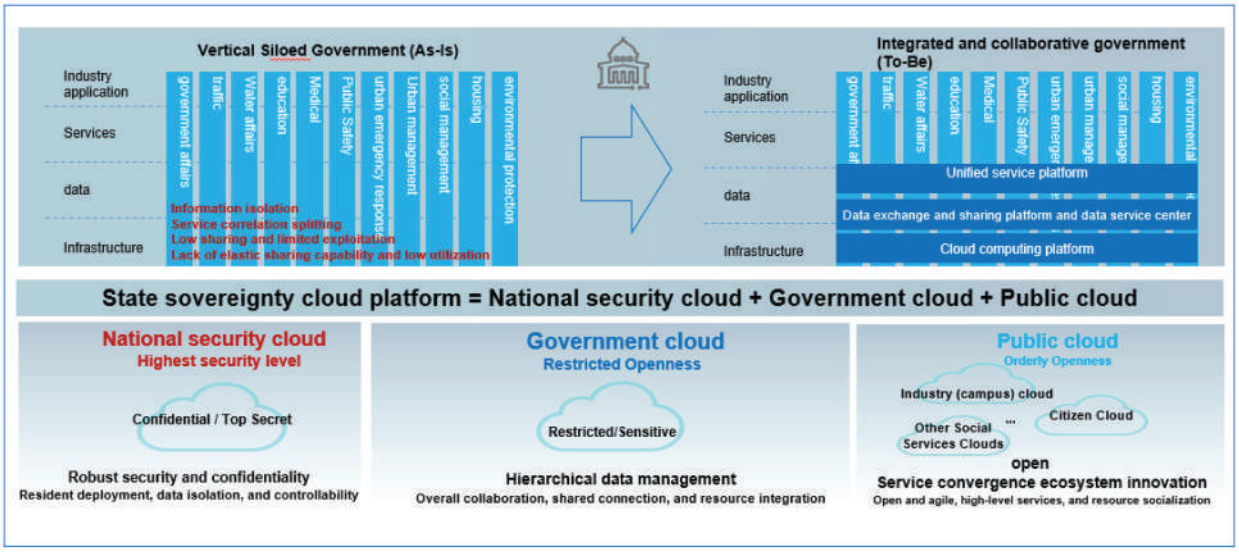
Also understanding from two perspectives as below:

- **Economic development perspective**:
  The legal, compliant and standard data flow is conducive to industry development. The government takes the lead in establishing management and monetization mechanisms to create value by providing data services and better support the healthy and rapid development of the digital economy.
- **Cyber security perspective**:
  The government takes the lead in implementing "local storage + cross-border supervision" for sensitive data based on data classification and classification, and establishes a monitoring mechanism, audit standards, security standards, and certification system.

2. **Government-led, industry-participated, national sovereignty cloud = national security cloud + Government cloud + public cloud, and cloud-cloud collaboration.**
   The governments take the lead and the industry participates in building a national sovereignty cloud platform. The advantages are as follows:
   - The national sovereignty cloud platform aims to build and share resources. The national security cloud, e-Government cloud, public cloud, and cloud-cloud collaboration feature maximizes efficiency, minimizes energy consumption, and effectively improves national digital economy competitiveness.
   - Government-led construction aggregate national value data, develop critical apps and cultivate talent, maintain national digital competitiveness and overtake others.

- Support underdeveloped regions, SMEs, and vulnerable groups to bridge the digital divide (Resource subsidy, capability enablement, skill training...).

Figure 18: State sovereignty cloud platform = National security cloud + Government cloud + Public cloud



Source: PIKOM Joint Working Group,2022Q4

» Vertical siloed Government:

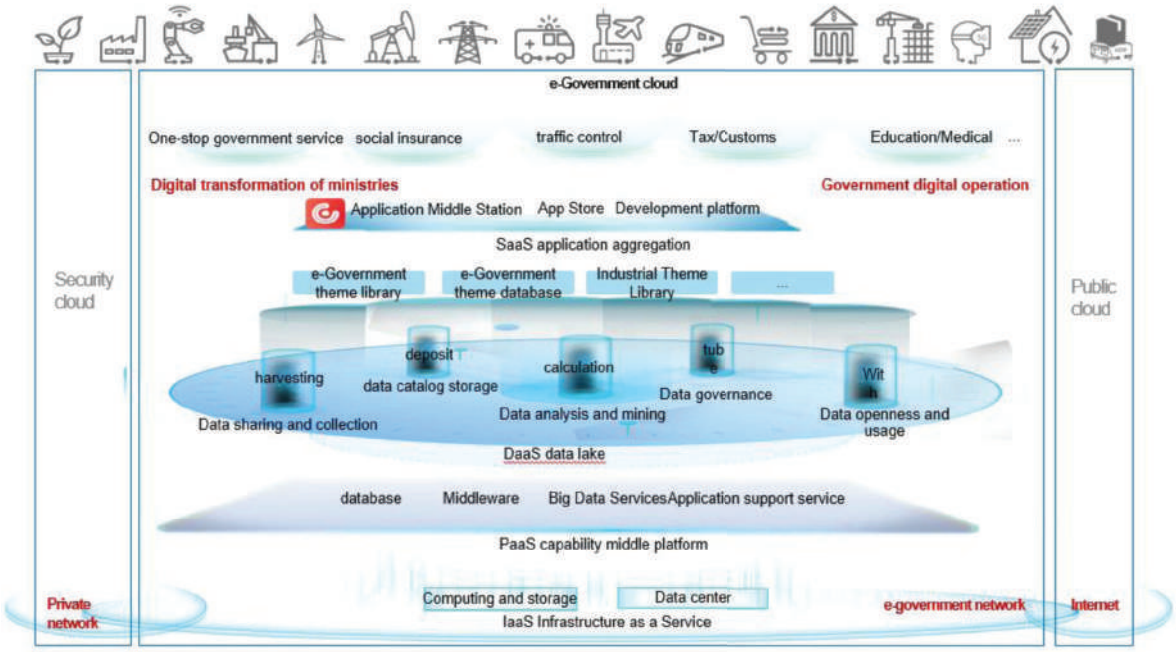
- Isolated information
- Service correlation splitting
- Low sharing and limited exploitation
- Lack of elastic sharing capability and low utilization

» Integrated and collaborative government:

- Unified service platform
- Data exchange and sharing platform and data service center
- Computing platform

3. The government accelerates the cloudification of government affairs, digital transformation of ministries, government digital operations, and promotes the digital transformation of industries.

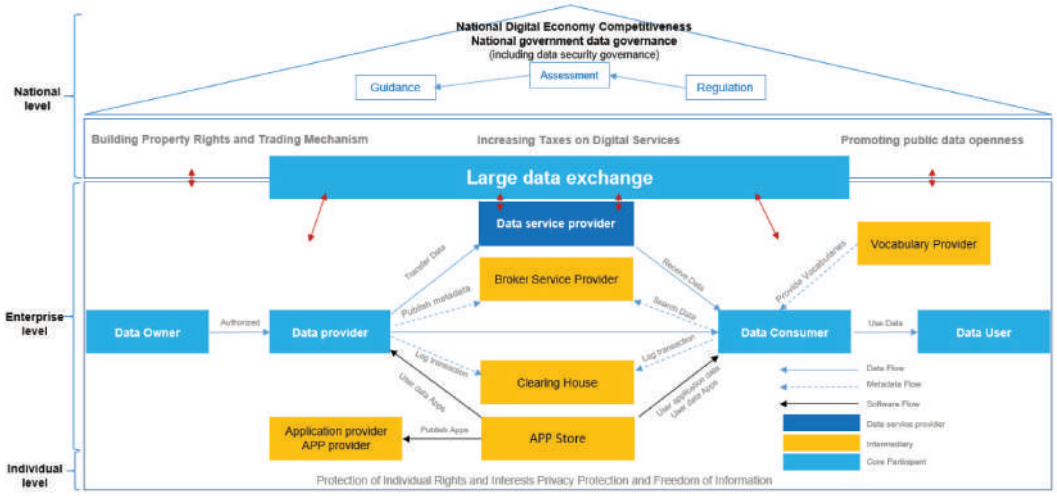
Figure 19: Digital Government



Source: PIKOM Joint Working Group,2022Q4

4. **The governments take the lead in setting up management and monetization mechanisms to create value through data services and increase the tax on digital services.**

Figure 20: Data management and monetization mechanisms



Source: PIKOM Joint Working Group,2022Q4

» **Vocabulary provider**:
Offer "vocabularies" such as ontologies, reference data models and metadata elements, which can be used to annotate and describe datasets.

» **Property rights and transaction mechanism**:
refers to the definition of data property rights and\relevant provisions of data transaction mechanism, such as the exclusive data property rights and the income sharing system of data as assets.

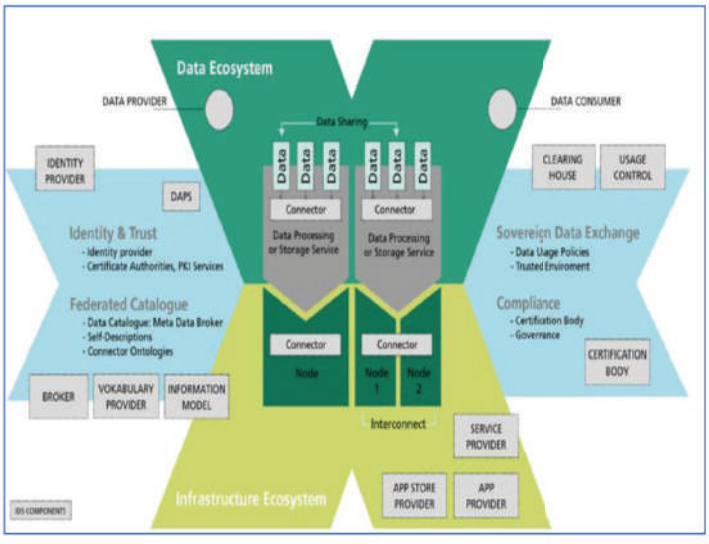
» **Digital service tax**:
refers to the tax provision for digital services, such as search engines, placement of targeted advertisements on digital interfaces, and provision of digital interface intermediary services to users.

» **Government public data openness**:
refers to the openness of data held by public sector institutions at all levels of government and organizations that are mainly funded by or under the control of public authorities.

Europe Use Case:
Creating business value through data services based on the data sovereignty cloud and IDS rules

The combined architecture of GAIA-X and IDS[72] supports and enables data spaces and advanced intelligent services for building vertical industries. GAIA-X focuses on sovereign cloud services and cloud infrastructure, while IDS focuses on data and data sovereignty. GAIAX interacts with IDS with three main tasks: sovereign data storage, trusted data use, and interoperable data exchange. In this way, GAIA-X is based on a data strategy developed in Europe to support smart data applications and innovation across industries. To this end, GAIA-X and IDS complement each other to ensure end-to-end data value chain sovereignty in the cloud and data federation ecosystem.

Figure 21: Mapping of IDS Components into the GAIA-X Architecture



[72] GAIA-X and IDS, https://internationaldataspaces.org/publications/most-important-documents/

The IDS Connector is responsible for the exchange of data, as it executes the complete data exchange process from and to the internal data resources and enterprise systems of the participating organizations. It is important to note that the data is transferred between the Connectors of the Data Provider and the Data Consumer (peer-to-peer network concept). The Connector architecture uses application container management technology to ensure an isolated and secure environment for individual data services.

The IDS Connector, one of the International Data Spaces' core components, connects industrial data clouds, as well as individual enterprise clouds, on-premises applications and individual, connected devices and therefore provides the technical access to an IDS ecosystem. It provides metadata to the IDS Broker as specified in the Connector self-description, e.g. technical interface description, authentication mechanism, exposed data sources, and associated data usage policies.

The IDS Connector is responsible for data exchange because it performs the complete data exchange process between the participating organizations' internal data resources and enterprise systems. It should be noted that data is transferred between the connector of the data provider and the data consumer (the peer-to-peer network concept). The Connector architecture uses application container management technology to ensure an isolated and secure environment for individual data services.

The IDS connector is one of the core components of the international data space, connecting industrial data clouds, individual enterprise clouds, on-premises applications, and individual connected devices, thus providing technical access to the IDS ecosystem. It provides IDS Broker with metadata specified in the connector read-me, such as technical interface descriptions, authentication mechanisms, exposed data sources, and associated data usage policies.

The Identity Provider provides an authentication service for all IDS participants. It offers a service to create, maintain, manage, monitor, and validate identity information of and for participants in the IDS. This is of particular importance for the network of trust in the IDS.

Identity providers provide authentication services for all IDS participants. It provides a service for creating, maintaining, managing, monitoring, and verifying the identity of participants in an IDS. This is particularly important for trust networks in IDS.

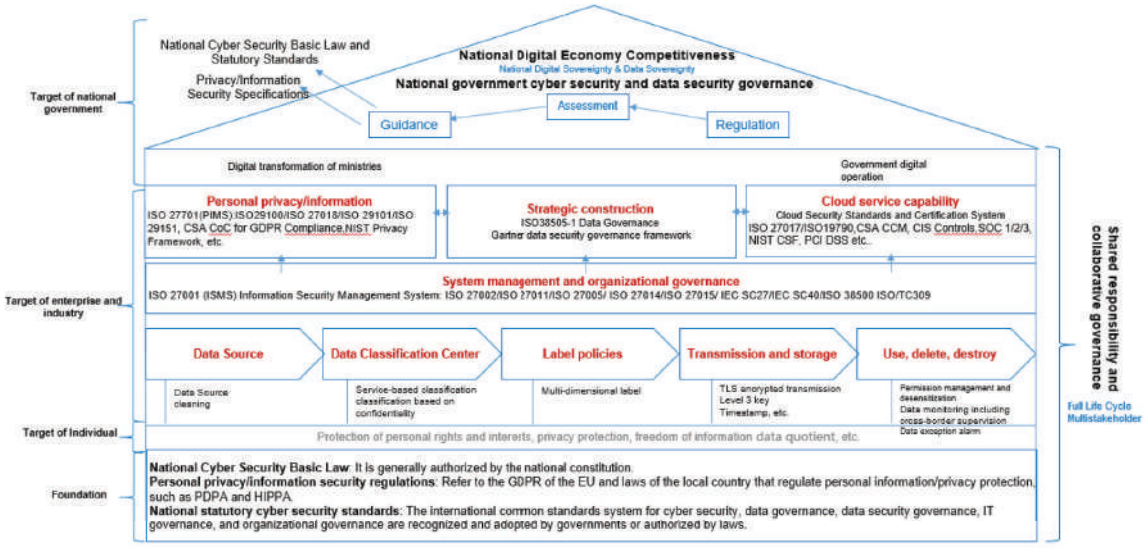
Intermediaries are Broker Service Provider, Clearing House, App Store Provider, App Provider, and Vocabulary Provider. For data exchange, the Data Provider makes metadata available via the IDS Broker. A Data Consumer can search this metadata for a dataset that fits their requirements. If the terms and conditions of the Data Provider match the needs of the Data Consumer, data exchange can take place. For this instance, the Connector logs the data transaction and sends the data record to the Clearing House. Additionally, Data Apps can further process the exchanged data. Those Data Apps are available in an App Store. They are deployed within the IDS Connector to facilitate data processing workflows. To annotate and describe datasets, specific vocabularies are offered by the Vocabulary Provider.

Intermediaries are broker service providers, clearing houses, app store providers, app providers, and data rule providers. For data exchange, the data provider provides metadata through IDS Broker. Data consumers can search this metadata for data sets that meet their requirements. Data exchange may be performed if the terms and conditions of the data provider meet the needs of the data consumer. For this instance, the connector logs the data transaction and sends the data record to the clearing house. In addition, the data application can further process the exchanged data. These data applications are available in the App Store. They are deployed in the IDS connector to facilitate the data processing workflow. To annotate and describe data sets, data rule providers provide specific vocabularies.

5.1 Governments take the lead in establishing a regulatory mechanism, audit standards, security standards and certification system.

Malaysia Data Security Governance Framework could be considered as below:

Figure 22: Malaysia Data Security Governance Framework



Source: PIKOM Joint Working Group,2022Q4

We also support and recognize the importance of adopting typical and international data security governance standards as below:

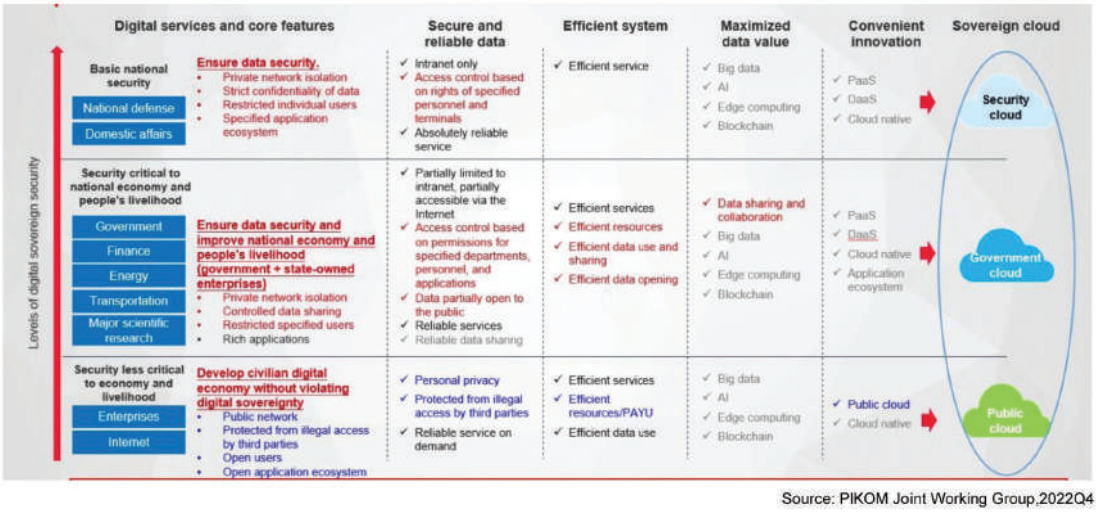
1) Standards of strategic construction such as ISO38505-1 and etc.;
2) Standards of personal privacy/information such as ISO 27701(PIMS):ISO29100/ISO 27018/ISO 29101/ISO 29151, CSA CoC for GDPR Compliance, NIST Privacy Framework and etc;
3) Standards of cloud service security such as ISO 27017/ISO19790, CSA CCM, CIS Controls, SOC 1/2/3, NIST CSF, PCI DSS and etc.;
4) Standards of system management and organizational governance such as: ISO 27001/ISO 27002/ISO 27011/ISO 27005/ ISO 27014/ISO 27015/COBIT 2019 for Information Security/ IEC SC27/IEC SC40/ISO 38500 ISO/TC309 and etc.

as it can use these standards as Malaysia Data Security Governance Framework to standardize cloud service provider (CSPs), cloud service customer (CSCs) and application software as a service (SaaS) provider that are effective and provide the highest level of security for subscribers. The most important benefit is the process by which all sectors play a role in driving trustworthy cloud service particularly collaboration to develop more secure cloud service using as a key guideline.

5.2 Governments take the lead in working out data classification and gradation rules and promote "data residence+ cross-border data transfer" for sensitive data.

The classification and gradation of data shall be based on the confidentiality and whether it harms the national security, public interests or the legitimate rights and interests of citizens or organizations.

Figure 23: Malaysia Data Security Governance Framework



Source: PIKOM Joint Working Group,2022Q4

It is recommended that the data of Malaysia be classified into three levels:

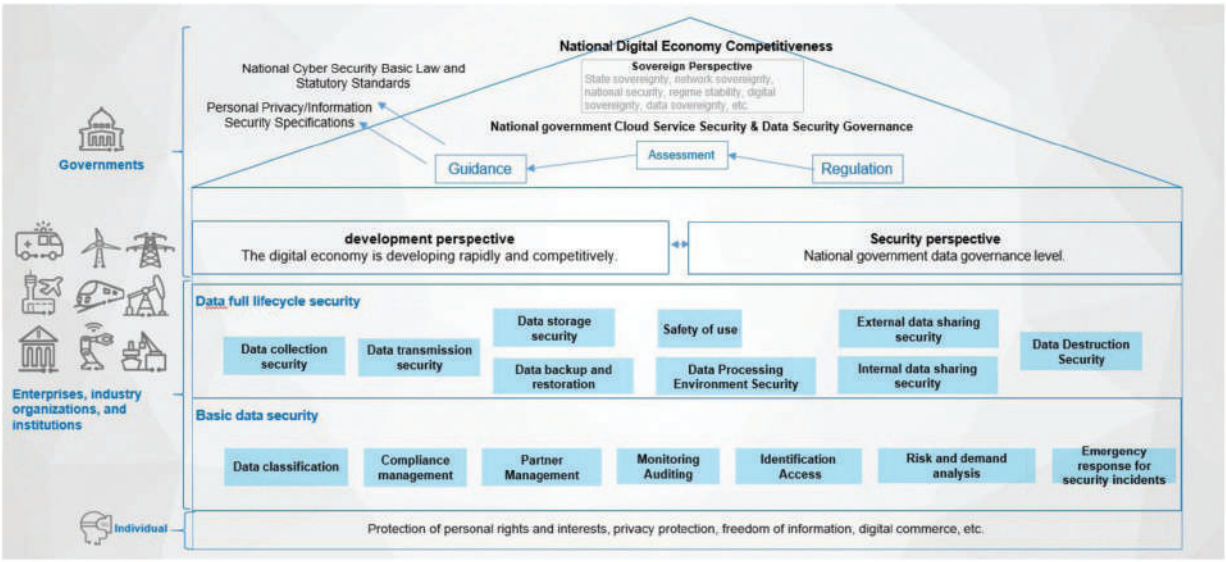
» **Classified data (Confidential/Secret/Top Secret)** includes international negotiation, defense, military, and national government data. National energy data, critical communications data, geographic information data and critical infrastructure data such as transportation, finance, telecommunications and power systems, personal data, population and health data, national budget and central financing data, statistical data, environmental meteorological data, marine environment data, enterprise registration data and other similar data. It includes confidential data whose disclosure, in whole or in part, would be detrimental to the national interest.

» **Sensitive/official data (official data) includes**: commercial data, general healthcare industry data, general education industry data, personal data, such as enterprise employee data, large health industry data, and any other data specified.

» **Unclassified data that can be disclosed Public information, databases, and other similar data that provides generally open and publicly accessible services.**

6. **The government takes the lead in building a multi-stakeholder collaborative governance model that adapts to the rapid development of the digital economy, and promotes the construction of basic data security and full-lifecycle data security at the enterprise level.**

Figure 24: Multi-stakeholder collaborative governance model



Source: PIKOM Joint Working Group,2022Q4

8 Afterword

We call on the entire ICT industry to invest more resources in creating comprehensive security and quality systems for digital application, digital technology, digital infrastructure, strategic construction, system management and organizational governance,personal privacy/information protection and reliable standards against which to assess them. We believe that the industry should develop globally-accepted, PPP (government and industry public and private partnership) -led, security standards, along with best practices, security assurance solutions, and compliance assessment systems. This will help establish a fair and consistent environment where all parties can respond to the challenges of cyber security together, achieve shared devopment and benefit together.

UN General Assembly First Committee Resolutions included “A community of shared future for humankind in Cyber Space” into “Developments in the Field of Information and Telecommunications in the Context of International Security” which were adopted on November 2022.

A community of shared future for humankind in cyber space is an indispensable part of a global village of shared future. The biggest vulnerability is a closed system. Collaboration is more effective than any encryption. Innovation trumps any firewall. Standards are the measure of trust. A sound ecosystem is our best protection.

Annex A

(Normative)

Normative references

Item	Terms /Standards	Title and Source
1	Global Industry Vision Exploring the Intelligent World 2030	https://www-file.huawei.com/-/media/CORP2020/pdf/giv/Intelligent_World_2030_en.pdf
2	ASEAN-Cybersecurity-Cooperation-Paper-2021-2025,	https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
3	ISO/IEC 18038:2020	ISO/IEC 18038:2020 Information technology — Computer graphics, image processing and environmental representation— Sensor representation in mixed and augmented reality, https://www.iso.org/standard/70720.html
4	ISO/IEC 18039:2019	ISO/IEC 18039:2019 Information technology — Computer graphics, image processing and environmental data representation — Mixed and augmented reality (MAR) reference model, https://www.iso.org/standard/30824.html
5	IEEE P2048	IEEE P2048 Standard for Augmented Reality on Mobile Devices: General Requirements for Software Framework, Components, and Integration, https://standards.ieee.org/ieee/2048.101/10390/
6	IEEE P3141	IEEE P3141 Standard for 3D Body Processing, https://standards.ieee.org/ieee/3141/10825/
7	ISO/IEC 21823-1:2019	ISO/IEC 21823-1:2019 Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework, https://www.iso.org/standard/71885.html
8	ISO/IEC 21823-2:2020	ISO/IEC 21823-2:2020 Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability, https://www.iso.org/standard/80986.html
9	ISO/IEC 21823-3:2021	ISO/IEC 21823-3:2021 Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability, https://www.iso.org/standard/83752.html
10	ISO/IEC 21823-3:2021	ISO/IEC 21823-3:2021 Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability, https://www.iso.org/standard/84773.html
11	ETSI SR 003 680	ETSI SR 003 680 Guidelines for Security, Privacy and Interoperability in IoT System Definition;A Concrete Approach, https://www.etsi.org/deliver/etsi_sr/003600_003699/003680/01.01.01_60/sr_003680v010101p.pdf
12	ETSI EN 303 645	ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
13	OWASP IoT verification standard	OWASP IoT verification standard, https://owasp.org/www-project-iot-security-verification-standard/
14	ISO/IEC JTC 1/SC 37	ISO/IEC JTC 1/SC 37 Biometrics, https://www.iso.org/committee/313770.html
15	ISO 62304	ISO 62304 Medical device software — Software life cycle processes, https://www.iso.org/standard/38421.html
16	ISO 14971	ISO 14971 Medical devices — Application of risk management to medical devices, https://www.iso.org/standard/72704.html
17	ISO/IEC JTC 1/SC 42 (Series)	ISO/IEC JTC 1/SC 42 (Series) Artificial intelligence, https://www.iso.org/committee/6794475.html
18		Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence, https://www.iso.org/standard/77608.html
19	ISO/IEC 20546:2019	ISO/IEC 20546:2019 Information Technology-Big Data-Overview and vocabulary, https://www.iso.org/standard/77608.html
20	ISO/IEC TR 20547:2020	ISO/IEC TR 20547:2020 Information Technology-Big data reference architecture, https://www.iso.org/standard/71275.html
21	IEEE BDGMM	IEEE BDGMM BIG DATA GOVERNANCE AND METADATA MANAGEMENT: STANDARDS ROADMAP, https://standards.ieee.org/wp-content/uploads/import/governance/iccom/bdgmm-standards-roadmap-2020.pdf
22	ITU-T SG16 Q22	ITU-T SG16 Q22 Multimedia aspects of distributed ledger technologies and e-services, https://www.itu.int/en/ITU-T/studygroups/2017-2020/16/Pages/q22.aspx
23	TC590	TC590 National Technical Committee for Standardization of Blockchain and Distributed Accounting Technology, https://std.samr.gov.cn/search/orgDetailView?tcCode=TC590
24	ISO/IEC TR 23188:2020	ISO/IEC TR 23188:2020 Information Technology-Cloud computing-Edge computing landscape, https://www.iso.org/standard/74846.html
25	ISO/IEC JTC 1/SC 38 (Series)	ISO/IEC JTC 1/SC 38 (Series) Cloud computing and distributed platforms, https://www.iso.org/committee/601355.html
26	3GPP Release15/16/17/18	3GPP Release15/16/17/18, https://www.3gpp.org/specifications-technologies/releases
27	3GPP TS 33.813	3GPP Study on security aspects of network slicing enhancement TS 33.813, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3541
28	GSMA 5G CKB	GSMA 5G CKB, https://www.gsma.com/security/5g-cybersecurity-knowledge-base/ Knowledge Base
29	ITU-T SG17 X.5G sec-guide	ITU-T work programme SG17 X.5G sec-guide, https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15006
30	NESAS|SCAS	NESAS|SCAS, https://www.gsma.com/security/network-equipment-security-assurance-scheme/
31	ISO/IEC 27017:2015	ISO/IEC 27017:2015 Information Technology-Security Techniques-Code of practice for information security controls based on ISO/IEC 27002 for cloud services, https://www.iso.org/standard/43757.html
32	ISO/IEC 19790:2012	ISO/IEC 19790:2012 Information Technology-Security techniques-Security requirements for cryptographic modules, https://www.iso.org/standard/52906.html
33	ISO/IEC 27034-1:2011	ISO/IEC 27034-1:2011 Information technology-Security techniques-Application security — Part 1: Overview and concepts，https://www.iso.org/standard/44378.html
34	Cloud Controls Matrix (CCM)	Cloud Controls Matrix (CCM), https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Annex A

(Normative)

Normative references

35	CIS	CIS Critical Security Controls Version 8, https://www.cisecurity.org/controls/v8
36	SOC 1/2/3	SOC 1/2/3, https://www.aicpa.org/cpe-learning/course/soc--for-cybersecurity-certificate-program
37	NIST CSF	NIST CSF, https://www.nist.gov/cyberframework
39	ISO/IEC 38505-1:2017	ISO/IEC 38505-1:2017 Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data, https://www.iso.org/standard/56639.html
40	ISO/IEC 27001:2022	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection- Information security management systems-Requirements, https://www.iso.org/standard/82875.html
41	ISO/IEC 27002:2022	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, https://www.iso.org/standard/75652.html
42	ISO/IEC 27011:2016	ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations, https://www.iso.org/standard/64143.html
43	ISO/IEC 27005:2018	ISO/IEC 27005:2018 Information technology-Security techniques -Information security risk management, https://www.iso.org/standard/75281.html
44	ISO/IEC 27014:2020	ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security, https://www.iso.org/standard/74046.html
45	COBIT	COBIT,https://www.isaca.org/resources/cobit
46	ISO/IEC JTC 1/SC 27	ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, https://www.iso.org/committee/45306.html
47	ISO/IEC JTC 1/SC 40	ISO/IEC JTC 1/SC 40 IT service management and IT governance, https://www.iso.org/committee/5013818.html
48	ISO/IEC 38500:2015	ISO/IEC 38500:2015 Information technology — Governance of IT for the organization,https://www.iso.org/standard/62816.html
49	ISO/TC 309	ISO/TC 309 Governance of organizations, https://www.iso.org/committee/6266703.html
50	ISO/IEC 27701:2019	ISO/IEC 27701:2019(en) Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en
51	ISO/IEC 29100:2011	ISO/IEC 29100:2011 Information technology-Security techniques-Privacy framework, https://www.iso.org/standard/45123.html
52	ISO/IEC 27018:2019	ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, https://www.iso.org/standard/76559.html
53	ISO/IEC 29151:2017	ISO/IEC 29151:2017 Information technology-Security techniques-Code of practice for personally identifiable information protection, https://www.iso.org/standard/62726.html
54	ISO/IEC 29101:2018	ISO/IEC 29101:2018 Information technology-Security techniques-Privacy architecture framework, https://www.iso.org/standard/75293.html
55	CSA CoC for GDPR Compliance	CSA CoC for GDPR Compliance, https://cloudsecurityalliance.org/privacy/gdpr/code-of-conduct/
56	NIST Privacy Framework	NIST Privacy Framework, https://www.nist.gov/privacy-framework
57	GAIA-X and IDS	GAIA-X and IDS, https://internationaldataspaces.org/publications/most-important-documents/
58	Korea K-ISMS	Korea K-ISMS, https://isms.kisa.or.kr/main/isms/intro/
59	Singapore MTCS	Singapore MTCS,https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Media-Releases/2013/new-multi-tier-cloud-security-mtcs-standard-launched-in-singapore
60	Germany C5	Germany C5,https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html
61	China GB/T 22239-2019	China GB/T 22239-2019,https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=BAFB47E8874764186BDB7865E8344DAF
62	China GB/T 31168-2014	China GB/T 31168-2014, https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=6630D5BE60B49E0414EB951BC354618B
63	UAE G42	UAE G42, https://www.mubadala.com/en/what-we-do/g42
64	PCI DSS	PCI DSS, https://www.pcisecuritystandards.org/document_library/
65	OSPAR(Singapore)	OSPAR(Singapore), https://www.abs.org.sg/industry-guidelines/outsourcing
66	PCI 3DS	PCI 3DS,https://www.emvco.com/emv-technologies/3d-secure/
67	UICC and eUICC	UICC and eUICC,https://www.gsma.com/security/security-accreditation-scheme/
68	USA HIPAA	USA HIPAA, https://www.cdc.gov/phlp/publications/topic/hipaa.html
69	CPS certification audit	CPS certification audit, https://www.cdsaonline.org/cps-standard/
70	Trusted Information Security Assessment Exchange (TISAX)	Trusted Information Security Assessment Exchange (TISAX), https://www.vda.de/vda/en/news/publications/publication/vda-isa-catalogue-version-5.1
71	ISO 27799:2016	ISO 27799:2016 Health informatics-Information security management in health using ISO/IEC 27002, https://www.iso.org/standard/62777.html

PIKOM

PERSATUAN INDUSTRI KOMPUTER DAN MULTIMEDIA MALAYSIA
THE NATIONAL TECH ASSOCIATION OF MALAYSIA

E1-01-G, Empire Damansara,
No 2, Jalan PJU 8/8A, Damansara Perdana,
47820 Petaling Jaya, Selangor Darul Ehsan,
Malaysia

Tel: +6(03) 7622 0079
twitter.com/pikomict
facebook.com/MYPIKOM
linkedin.com/in/pikom

www.pikom.org.my