DIGITAL TRUST MODEL FOR DIGITAL PROSPERITY

Publication of

PIKOM

Document Name	Digital TRUST Model for Digital Prosperity
Summary	The document provides Digital TRUST Model for Digital Prosperity as a reference for all stakeholders to co-contribute to the life quality of the intelligent world 2030.
Version	V1.0
Release Date	*1/1/2024*

Contents

PROFESSOR
DR. MOHD NAZRI BIN KAMA
Personal Data Protection
Commissioner Malaysia

Foreword:

Safeguarding Trust, Fueling Prosperity in the Digital Age

In an era where the digital realm permeates every facet of our lives, the question of data privacy and cybersecurity looms large. It is a question that demands not just technical solutions, but a collaborative approach, a shared vision, and a global language. And within this complex landscape, the publication of the “Digital TRUST Model for Digital Prosperity” is a timely roadmap toward a safer, more prosperous digital future.

As Personal Data Protection Commissioner in Malaysia, I am acutely aware of the challenges and opportunities that accompany digital transformation. The book’s central thesis resonates deeply on the premise that cybersecurity risk is not an insurmountable obstacle, but rather, a hurdle to be tackled head-on. This is precisely the focus of the Malaysian government’s initiatives. We have embarked on an ambitious digital roadmap, prioritizing cybersecurity and data privacy as cornerstones.

The robust protection of personal data and meticulous compliance with Malaysia’s Personal Data Protection Act 709 can significantly bolster digital confidence within the nation’s cybersecurity ecosystem. This synergy arises from several key factors. Firstly, strong data protection measures reassure individuals that their online information is handled responsibly and securely, mitigating concerns about privacy breaches and misuse. These fosters trust in digital platforms and services, encouraging wider adoption and engagement. Secondly, adherence to Act 709’s stringent data governance procedures instills confidence in businesses and organizations operating within the digital realm. The Act’s emphasis on data security best practices, accountability, and transparency that minimizes the risk of cyberattacks and data breaches, safeguarding sensitive information and promoting a stable and reliable digital environment.

As individuals and organizations become more mindful of data privacy and security regulations, they are more likely to adopt secure practices and actively participate in collective efforts to combat cyber threats. This collaborative approach strengthens the overall cybersecurity posture of the nation, further bolstering digital confidence. In conclusion, the effective protection of personal data and strict compliance with Act 709 act as cornerstones for building a vibrant and trustworthy digital ecosystem in Malaysia, ultimately enhancing digital confidence for all stakeholders within the ecosystem of data protection.

“Digital TRUST Model for Digital Prosperity” goes beyond outlining technical solutions. It emphasizes the crucial role of shared responsibility and global collaboration. Let us navigate the digital landscape together, with innovation, collaboration, and a shared commitment to building a world where the promise of digital prosperity is realized for all.

PITI SRISANGNAM
Executive Director,
ASEAN Foundation

Foreword:

Embracing the Digital TRUST Model for a Prosperous GenAI World

Welcome to GenAI, the Singularity of the Digital Era

The year is 2030. We stand on the cusp of a new age, a world transformed by the ubiquitous presence of general-purpose artificial intelligence (AGI). This is the dawn of GenAI, a singularity where the unimaginable becomes ordinary. Imagine a world seamlessly connected, where everyday life unfolds through an intricate tapestry of cloud services woven by AGI. From the moment we wake to the gentle whisper of AI-powered assistants, to the effortless control of our homes with intuitive voice commands, to the seamless integration of work, leisure, and learning facilitated by AI-powered platforms, the GenAI era promises a future unimaginable just a decade ago.

Navigating the GenAI Landscape: Embracing Sustainability and Equity.

Yet, the promise of GenAI comes hand in hand with immense responsibility. Our interconnectedness demands a new awareness of the impact our actions have on the planet. We must foster a polycentric approach to environmental governance, where AI-driven technologies enable sustainable practices and radical reductions in energy and resource consumption. Our focus must shift beyond mere economic growth towards a future that prioritizes socio-economic sustainability and fosters unity with nature. We must move away from irresponsible consumption patterns and embrace social equity and justice as the cornerstones of a global society in equilibrium with its environment.

The Digital TRUST Model: A Blueprint for a Sustainable and Equitable GenAI World.

The Digital TRUST Model offers a powerful roadmap to navigate the complexities of GenAI. This model, with its emphasis on T: Technology & Talent, R: Shared Responsibilities, U: Unified Multi-Stakeholders' Collaboration, S: International Common Standardization, and T: Fair Digital Trade, provides a comprehensive framework for building a future that is prosperous, sustainable, and inclusive.

The Digital TRUST model recognizes that achieving GenAI's full potential requires a shared commitment from all stakeholders. From the development of ethical and responsible AI technologies to the promotion of digital literacy and data security, collective action is essential. By collaborating across sectors and borders, we can ensure that GenAI benefits all of humanity, bridging the digital divide and fostering a global community united in progress.

ASEAN Foundation and the Digital TRUST Model: Partnering for a Shared Future.

The ASEAN Foundation, where I serve as Executive Director, is committed to playing a vital role in shaping the future of GenAI within the ASEAN region. We actively promote digital knowledge, data analytics, and cybersecurity, empowering our people with the skills they need to thrive in the digital age. Through collaborations with all stakeholders, we aim to jointly build a people-centered ASEAN community that is strong, sustainable, and ready to embrace the opportunities of GenAI.

The future holds immense promise, but it also presents significant challenges. By embracing the Digital TRUST model and working together, we can ensure that GenAI leads us towards a brighter future – a future where technology enhances our lives, protects our planet, and empowers all of humanity to flourish. The ASEAN Foundation and I stand alongside all stakeholders, ready to support initiatives that will make this vision a reality. Let us step forward together, united in purpose, and build a prosperous and equitable GenAI world for all.

Congratulations to this timely and insightful book and I would like to thank the ASEAN Secretariat, Malaysia PDPD (Protection of Data Privacy Dept) and PIKOM for their professional guideline and contribution and the team of experts who worked on this project. We are confident that the Digital TRUST model will serve as a valuable guide as we navigate the exciting yet complex landscape of GenAI. We look forward to collaborating with all stakeholders to ensure that GenAI brings about a brighter future for all.

ONG CHIN SEONG
Chairman, PIKOM

Foreword:

Unlocking Digital Prosperity Through Trust and Collaboration

I am thrilled to welcome the arrival of “Digital TRUST Model for Digital Prosperity” book as cybersecurity is a critical cornerstone of this digital future. Cyber risks pose a significant threat, but the book asserts that these risks are not insurmountable. By embracing appropriate technical measures, fostering innovation, and nurturing a skilled digital workforce, we can effectively mitigate these challenges and unlock the immense potential of the digital economy.

This is where industry players like ourselves, the very fabric of PIKOM, must take the lead. We are not merely bystanders in this digital transformation; we are active architects. We must champion the adoption of robust cybersecurity practices, invest in cutting-edge technology solutions, and actively cultivate a talent pool equipped with the skills needed to navigate the ever-evolving digital landscape.

The book’s emphasis on shared responsibility resonates deeply with PIKOM’s core values. Digital ecosystem development is not a solo endeavor; it requires a collective effort, a symphony of voices from diverse stakeholders. We, the industry, must work hand-in-hand with government agencies, educational institutions, and civil society to create a comprehensive ecosystem that fosters trust and collaboration.

Furthermore, the book’s call for globally accepted standards in digital trade strikes a critical chord. Fair trade in the digital realm is essential for ensuring a level playing field where innovation and competition flourish. PIKOM actively advocates for such standards, recognizing that a fragmented digital landscape hinders not just economic growth, but also the very fabric of trust and cooperation that underpins a prosperous digital future.

“Digital TRUST Model for Digital Prosperity” is more than just a book; it is a clarion call to action. It challenges us, the industry, to rise to the occasion, to embrace our role as active participants in shaping a secure, inclusive, and prosperous digital future. We must lead by example, championing best practices, nurturing talent, and fostering collaboration.

1 Normative references

The following normative references are indispensable for the application of this Digital TRUST Model for Digital Prosperity. 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

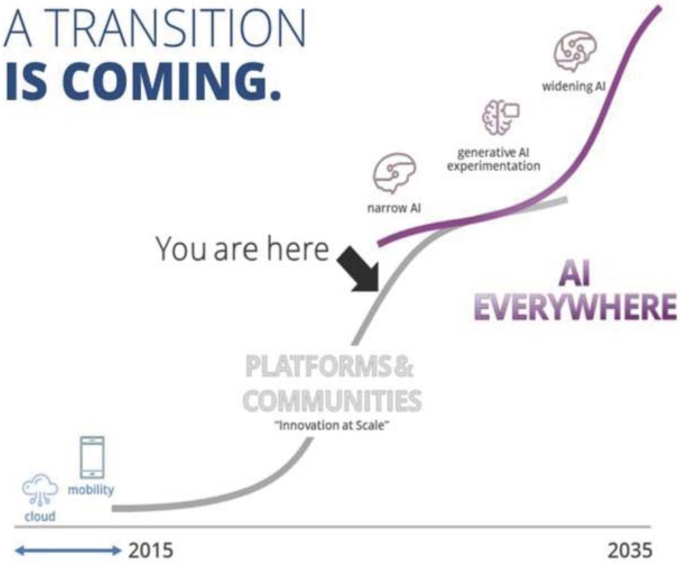
AI	Artificial intelligence
GenAI	Generative AI
GIV	Global Industry Vision
eVTOL	Electric vertical take-off and landing
MSP	Multi-Stakeholder Partnerships
GDPR	General Data Protection Regulation
ISC2	International Information Systems Security Certification Consortium
PEC	Privacy-Enhancing Computation
TEE	Trusted Execution Environment
STEM	Science, Technology, Engineering, and Mathematics
GSMA	Groupe Speciale Mobile Association
GSMA Mobile CKB	GSMA Mobile Cybersecurity Knowledge Base
MNOs	Mobile Network Operators
NESAS	Network Equipment Security Assurance Scheme
NE	Network Element
OIC-CERT	Organization of The Islamic Cooperation Computer Emergency Response Team
OSI	Open System Interconnection
3GPP	3rd Generation Partnership Project
ETSI	European Telecommunications Standards Institute
ENISA	European Union Agency for Cybersecurity
C2C-CC	CAR 2 CAR Communication Consortium
W3C	World Wide Web Consortium
RIDE MADANI	RCEP Innovation and Digital Ecosystem MADANI
FTA	Free Trade Agreement
DEPA	Digital Economy Partnership Agreement
DEFA	Digital Economy Framework Agreement
DEAs	Digital Economy Agreements
GAIA-X	A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem, EU Sovereignty Cloud
IDS	International Data Spaces
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
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

4 Outlook for Intelligent World 2030

4.1 We are at Singularity of Digital Era: GenAI

Artificial Intelligence (AI) has become mainstream and will be embedded everywhere. Economies need to adjust their policies to facilitate the development of an Intelligent Economy in an Intelligent World. Proliferation of data and investment in analytics and AI are transforming the world towards an Intelligent World. GenAI is a game changer with significant impact on the economy and society to drive >18% increase in productivity and output.

Figure 1 Singularity: GenAI

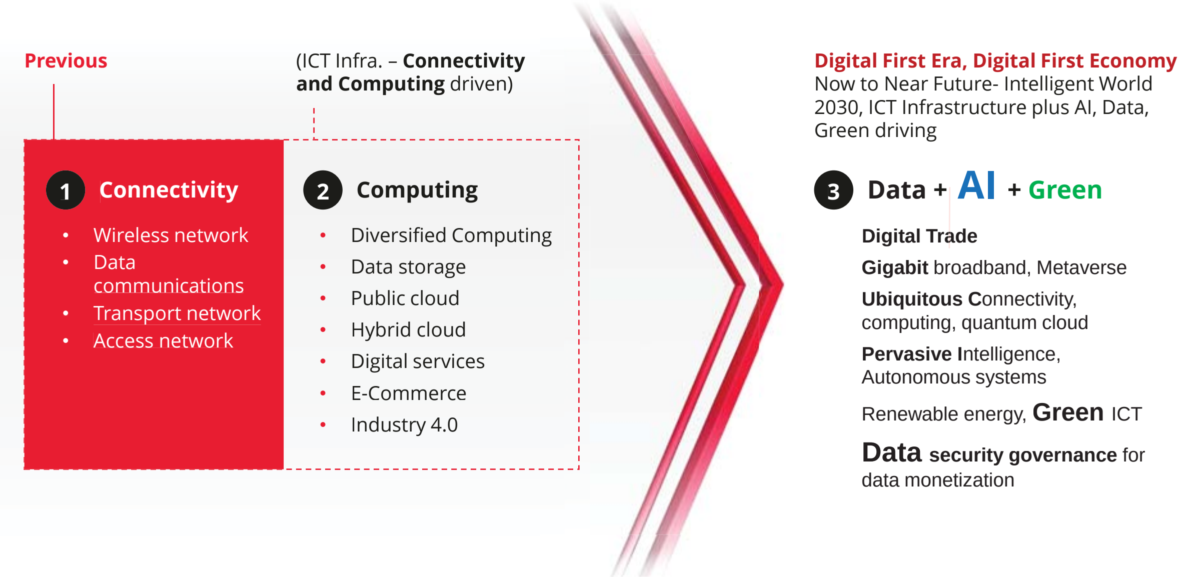


GenAI democratizes the use of AI, facilitating innovation and driving new economic opportunities for industry and public sector services and capabilities.

- Society and all workers can use AI without code
- Assist and guide workers generating creative content, not just data
- Constantly learning and improving
- New software models creating future software and services startups
- Region specific localization creates domestic companies

Intelligent World 2030 is evolving from "Connectivity and Computing" to"Data+AI+Green ".

Figure 2 Data+AI+Green Era



Previous

(ICT Infra. – **Connectivity and Computing** driven)

1 **Connectivity**

- Wireless network
- Data communications
- Transport network
- Access network

2 **Computing**

- Diversified Computing
- Data storage
- Public cloud
- Hybrid cloud
- Digital services
- E-Commerce
- Industry 4.0

Digital First Era, Digital First Economy
Now to Near Future- Intelligent World 2030, ICT Infrastructure plus AI, Data, Green driving

3 **Data + AI + Green**

Digital Trade

Gigabit broadband, Metaverse

Ubiquitous Connectivity, computing, quantum cloud

Pervasive Intelligence, Autonomous systems

Renewable energy, **Green** ICT

Data security governance for data monetization

[1] Digital First Economy, https://www2.abaconline.org/assets/2022/Publications/Digital%20First%20Economy.pdf

With high speed and low latency gigabit broadband, there are new business models and opportunities for people and businesses. The way people and businesses consume and produce will also change. The increase in bandwidth, speed, and stability will generate new income streams for people, such as enabling professional services to be delivered digitally through video and augmented reality/virtual reality (AR/VR) with the aid of AI systems and the Internet of Things (IoT) devices. The gig economy is no longer limited to a lower value and skilled jobs and a realm of contractors and freelancers. It is no longer tied to digital content that can only be delivered via digital devices with a screen. The anywhere and anytime immersive physical and digital-blended experiences and services will give rise to the metaverse.

AI augmentation will become an essential productivity factor to unlock additional value in regional and national economies as we move beyond automation-driven productivity to autonomous intelligence-enabled productivity. This will result in a rise in startups with business models centered around AI and data as their core, leveraging the ubiquitous computing and quantum cloud to challenge and transform traditional businesses. This will likely drive the transformation of the entire industry and the emergence of new industry sectors that are digitally based services or products, with digital content, creativity as a differentiator, and AI and autonomous systems leveling the production playing field.

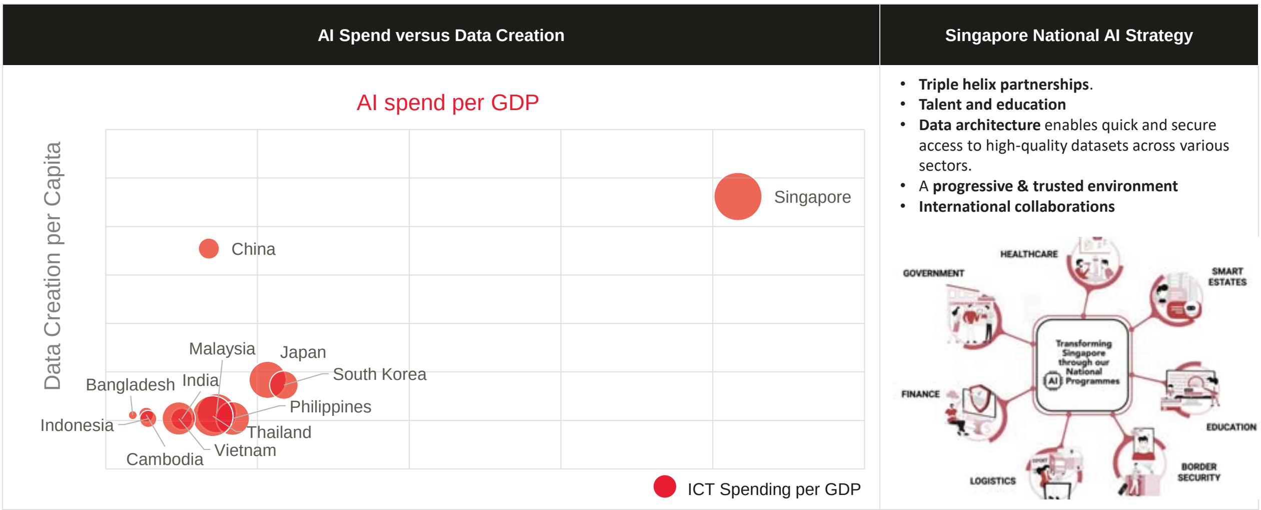
The increase in digital consumption and production will demand a greater energy supply. This supply needs to shift from traditional high carbon emission sources to renewable energy for this digital evolution to be sustainable. Clean technologies will be prioritized alongside ICT investments as regional and national communities and organizations are required to reduce their carbon footprint.

Data and information are not only a production input but also a final product that can be traded, sold, or function as further inputs to create other data products. As large volumes of data come into play, data governance for data monetization will be increasingly crucial for regional and national economies.

Use case: Singapore National AI Strategy

Digitalization will be key to create the data assets needed for AI and monetization. This is enabled by building the data architecture that is dependent on a robust digital connectivity, data sovereignty and cloud computing. AI spending unlocks the value of data for effective and efficient monetization.

Figure 3 Singapore National AI Strategy



AI Spend versus Data Creation

Singapore National AI Strategy

- **Triple helix partnerships**.
- **Talent and education**
- **Data architecture** enables quick and secure access to high-quality datasets across various sectors.
- A **progressive & trusted environment**
- **International collaborations**

Sources: Elaborated from DFE 1.0 & 2.0, IDC

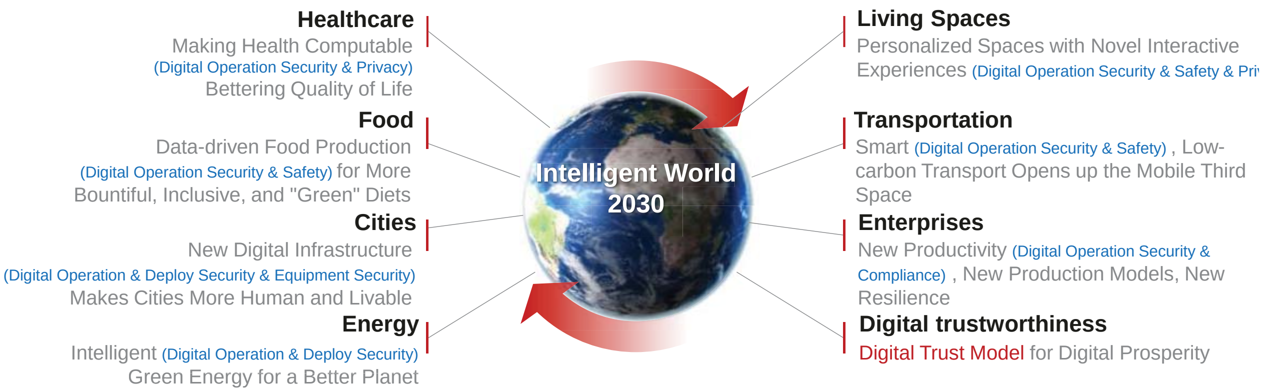
4.2 What is Intelligent World 2030

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 transformations, digital operations, data & AI security and trustworthy 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 4 Intelligent World 2030



Intelligent World 2030

Healthcare
Making Health Computable (Digital Operation Security & Privacy) Bettering Quality of Life

Food
Data-driven Food Production (Digital Operation Security & Safety) for More Bountiful, Inclusive, and "Green" Diets

Cities
New Digital Infrastructure (Digital Operation & Deploy Security & Equipment Security) Makes Cities More Human and Livable

Energy
Intelligent (Digital Operation & Deploy Security) Green Energy for a Better Planet

Living Spaces
Personalized Spaces with Novel Interactive Experiences (Digital Operation Security & Safety & Pri

Transportation
Smart (Digital Operation Security & Safety) , Low-carbon Transport Opens up the Mobile Third Space

Enterprises
New Productivity (Digital Operation Security & Compliance) , New Production Models, New Resilience

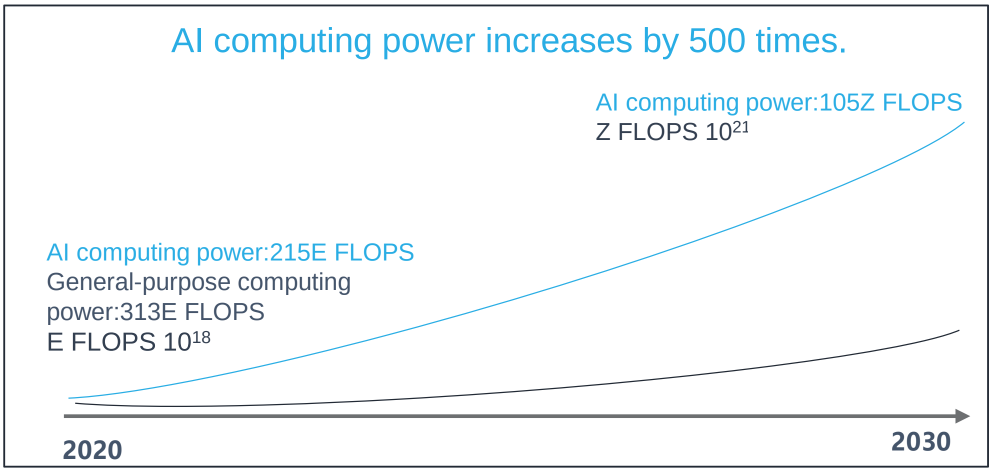
Digital trustworthiness
Digital Trust Model for Digital Prosperity

# of connections worldwide	General-purpose computing power (FP32)	AI computing power (FP16)	Cloud services as % of total enterprise application expenditure	Share of renewable energy in global electricity generation
200 bn	3.3Z FLOPS, 10x ⬆	105Z FLOPS, 500x ⬆	87%	50%

- **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.

  GIV (Global Industry Vision) predictions by 2030:
  - AI computing power (FP16): **105Z FLOPS**, a **500x** increase over 2020
  - Global general computing power (FP32): **3.3Z FLOPS**, a **10x** increase over 2020

Figure 5 Ubiquitous Computing



[2] Global Industry Vision Exploring the Intelligent World 2030, https://www-file.huawei.com/-/media/CORP2020/pdf/giv/Intelligent_World_2030_en.pdf

- **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.

  GIV predictions for 2030:
  - There will be **200 billion** connections worldwide.
  - **1YB** of data will be generated annually worldwide, a **23-fold** increase over 2020.

- **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.

  GIV predictions by 2030:
  - There will be **1.6 billion** fiber broadband subscribers.
  - **23%** of homes will have access to **10 gigabit** fiber broadband.

- **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.

  GIV predictions by 2030:
  - **50%** of new vehicles sold will be electric vehicles.
  - Whole-vehicle computing power will exceed **5,000TOPS**.

- **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.

  GIV predictions by 2030:
  - **40%** of companies will have access to 10 gigabit Wi-Fi networks.

- **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.

GIV predictions by 2030:

- Every **10,000** workers will work with **390** robots.
- One million companies are expected to build their own 5G private networks (including virtual private networks).
- Cloud services are forecast to account for **87%** of enterprises' application expenditures.
- AI computing will account for **7%** of a company's total IT investment.

- **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.

  GIV predictions by 2030:
  - Renewables will account for **50%** of all electricity generation globally.

- **Outlook for Digital Trust: Digital trust model for digital prosperity.**
  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. All cities are all-smart, all-optical, all-human, all connected, and all green…a world where 85 percent of all companies use unbreakable blockchain technology to protect personal identity and security and where more than half of all computing is "privacy enhanced" … a world where **digital trade** are as flexible and resilient as human minds under **digital trust model**.

  GIV predictions by 2030:
  - Privacy-enhanced computing technologies will be used in more than **50%** of computing scenarios.
  - **85%** of enterprises will adopt blockchain technology.

5 Digital TRUST Model

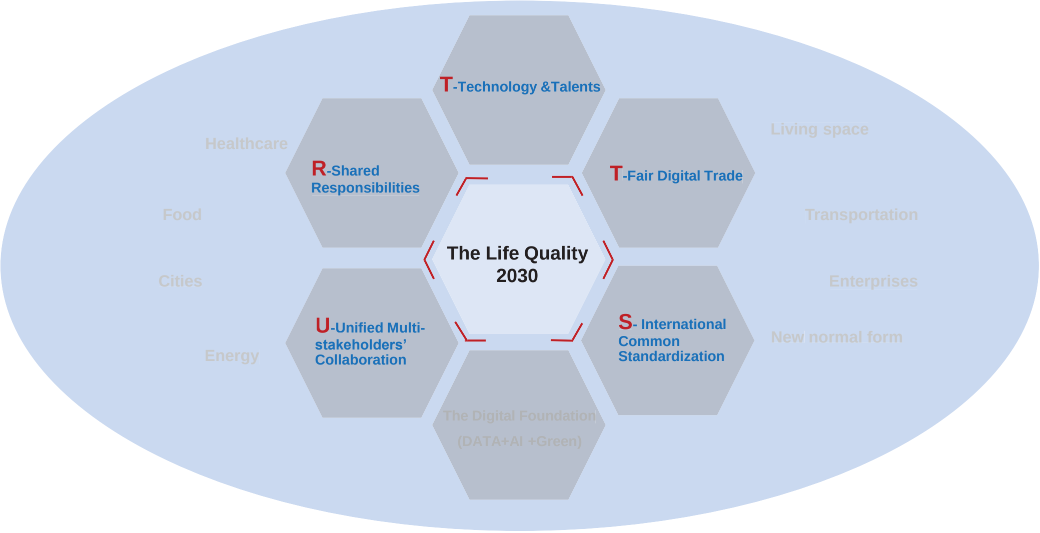
Creating digital trust is actually a process and must be done in a structured manner which brings together all representative stakeholder voices who are committed to unified standards and also willing to take part of the responsibility for establishing a cybersecurity ecosystem.

Therefore, a framework is essential for accommodating the dynamic nature of cybersecurity-newly emerging threats, policy evolution, technology developments plus changing economic and social factors. A framework must factor in policies, practices and procedures and support all organizations with protecting their assets via a process that includes identifying, assessing and managing potential disruptions.

Meanwhile, a framework must enable regions and nations to improve the competitiveness of the digital economy. And the ultimate purpose of framework is to improve the life quality in the intelligent real-time world where waits and delays, queues and paperwork, hassles and drudgery dissolve in almost instantaneous provision of goods and services when and where you need them most, where no one has to wait in lines for care, where cancer and pandemic alike are cancelled…a world turning data into food to solve world hunger in farms that become skyscraping factories unaffected by climate or scarcity of land, where people commute in self-driving cars that are colleges, opening up a new “third space” of mobile learning and entertainment, where the self-driving revolution engulfs the skies, with electric taxis of the air available at a whim, where cities are all-smart, all-optical, all-human, all connected, and all green, where companies are as flexible and resilient as human minds in new webs of digital trust.

Multi-Stakeholder Partnerships (MSP) bring together different societal players (public sector, private sector, civil society, academia) working together as equals, sharing risks, and combining unique resources and competencies to address challenges or exploit opportunities in ways that one cannot achieve alone to facilitate the development of sustainable frameworks. Based on all stakeholders’ contributions and the best industrial knowledge and practices above, we developed the **Digital TRUST Model**, to help build the cybersecurity ecosystem holistically centered on the life quality in the intelligent world 2030 as below:

Figure 6 Digital TRUST Model



5.1 T-Technology & Talents

Technical Base: Cybersecurity is rooted in technology. Cybersecurity risk can be appropriately governed by technical measures and mitigated by technical innovation.

In the business world, all interactions are ultimately based on trust, from market research to customer engagement, enterprise operations and management, and the supply chain. Now, digital technology is reshaping these interactions and new concepts such as the metaverse are emerging. Building digital trust has become one of the most important strategic goals for companies and other organizations. Interactions between organizations, between organizations and customers, and within organizations, are migrating to the digital world ever more quickly. Valuable digital assets are generated during these processes. However, the basis of these interactions, i.e., the trust, will be lost if information security is compromised or private information is leaked. As a result, business operations, business value (e.g., brand and market value), reputation, and public credibility will all be at risk. Digital trust is a complex system that covers a range of areas, including privacy, security, identity, transparency, data integrity and governance, and compliance. Let us first clarify the difference between data security, cyber security and privacy protection as below:

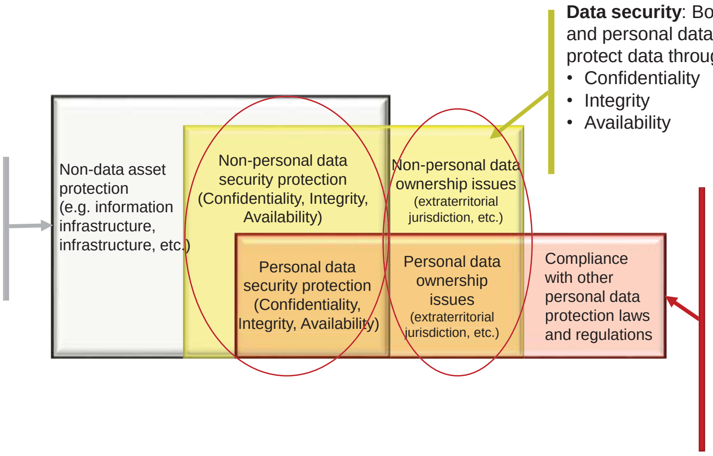
Cyber security: Build a cyber-centric security system to protect data and other assets (computing and IoT), including non-data assets and data assets.
Data security: Covers both non-personal and personal data and is designed to protect data throughout its lifecycle.

- 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 7 The difference between data security and cyber security and privacy


Non-data asset protection (e.g. information infrastructure, infrastructure, etc.)
Non-personal data security protection (Confidentiality, Integrity, Availability)
Non-personal data ownership issues (extraterritorial jurisdiction, etc.)
Personal data security protection (Confidentiality, Integrity, Availability)
Personal data ownership issues (extraterritorial jurisdiction, etc.)
Compliance with other personal data protection laws and regulations

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

- Confidentiality
- Integrity
- Availability

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

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

➢ Cyber security: Focus 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: Focus on protecting data against malicious attacks and being stolen data for illegal profit gain.

Therefore, the realization of digital trust must involve different dimensions and use a variety of technology tools, such as blockchain, privacy-enhancing technology, and artificial intelligence (AI). New technologies and new rules will help shape a trusted digital future.

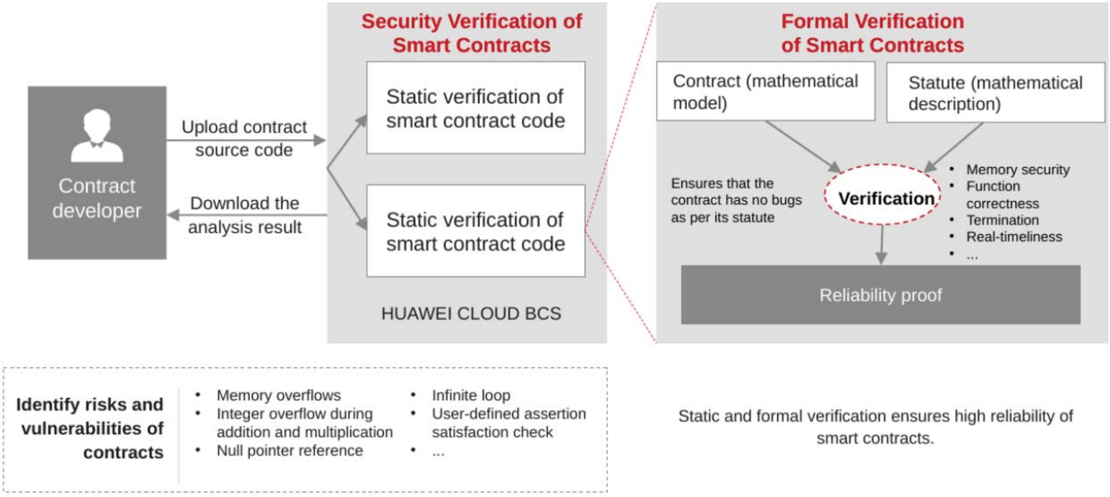
ICT talents and security & privacy talents are indispensable to enabling national digital economy development. Cyber security skill improvement and talent cultivation are common challenges facing by the Asia-Pacific region and even the world. The ISC2 (International Information Systems Security

Certification Consortium) Cybersecurity Workforce Study shows that the amount of global cybersecurity workforce estimated is 4.66 million, and there is a gap of more than 3.4 million cybersecurity workforce worldwide and more than 2.1 million in APAC. We call governments formulate the talent cultivation programme adapted to the digital era through government-enterprise talent cooperation mechanism regarding on new ICT, cyber security, privacy protection talents and data security governance talents as well as improvement of cyber security culture awareness education.

Use case:

1. **Smart contracts on the blockchain**

Figure 8 Typical Smart Contract Solution


Security Verification of Smart Contracts
Contract developer
Upload contract source code
Download the analysis result
Static verification of smart contract code
Static verification of smart contract code
HUAWEI CLOUD BCS
Formal Verification of Smart Contracts
Contract (mathematical model)
Statute (mathematical description)
Ensures that the contract has no bugs as per its statute
Verification
Memory security
Function correctness
Termination
Real-timeliness
...
Reliability proof
Identify risks and vulnerabilities of contracts
Memory overflows
Integer overflow during addition and multiplication
Null pointer reference
Infinite loop
User-defined assertion satisfaction check
...
Static and formal verification ensures high reliability of smart contracts.

Many companies are looking for solutions that enable contracts to be drafted and executed efficiently, and provide automated performance and neutral supervision. Smart contracts, executed on a blockchain, have been one of the most exciting areas of development in recent years. Smart contracts were first defined by Nick Szabo in 1994 as a set of promises, specified in digital form, including protocols within which the parties perform on these promises. Thus, a smart contract is a special type of agreement that creates, verifies, and enforces performance of obligations. However, smart contracts were only a theoretical concept until the introduction of blockchain, because the technology to create them did not exist. Blockchain-based smart contracts contain terms expressed in a digital form on a blockchain, and the recording and processing of these terms are completed on the blockchain. The code of the contract contains the obligations of the parties and all information relating to the transactions. The obligations are performed automatically when the set conditions are met, and no third parties are required. Blockchain technology allows information to be recorded and distributed, which ensures that the entire process, from contract storage and access to performance, is transparent, traceable, and non-tamperable. In addition, the decentralized technology that underpins smart contracts can help companies reduce operational costs, improve contract performance efficiency, and prevent third-party interference, which would make transactions more accurate and reliable. However, these same features of blockchain also create challenges to the widespread adoption of smart contracts. For example, if there are errors in the code of a smart contract, the errors cannot be corrected.

2. **Using AI to identify fraud and maintain organizational reputation and credibility**
   AI-based behaviors are increasingly humanlike. Therefore, some people may use AI for deception. It is difficult for humans and traditional technologies to distinguish fake video and audio created using digital technologies from legitimate audio and video such as “Face-swapping fraud sparks AI-powered crime”, “Deep fake APP causes fraud and privacy fears”, “AI Scam Alert!” and relevant recent hot AI powered fraud crimes cases.

[3] Cybersecurity Workforce Study 2023, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4

Figure 9 AI anti-fraud Solution

However, the solution to this malicious use of AI may come from AI itself. Neural networks for deep learning can be used to analyze natural language and images, and even to understand video and audio. This can allow us to distinguish between authentic and deep fake videos. AI can be used to detect differences between videos, or even slight differences in audio waves. It can thus identify whether a video or audio was composed using AI. Machine learning and API technology can be used to automate defense. In particular, discriminator algorithms and causal inference models can be used to automatically detect, assess, and remove fake information on the Internet, and trace it back to the data source to provide evidence for the prosecution of digital crimes.

3. **Privacy-enhancing computation**

In the era of big data, data is the new oil. But unlike oil, data will not be depleted. The value of data will be realized again and again in different scenarios and regions by all kinds of enterprises and organizations. However, data sharing presents new challenges to security and privacy. Data mining and analytics driven by machine learning is becoming increasingly prevalent. Sectors such as finance, healthcare, and retail in particular need to guarantee data privacy as they seek to mine data, obtain its value, and share it for collaboration. As data analytics and data warehouse environments become increasingly complex, traditional data desensitization technologies are no longer sufficient. Therefore, privacy-enhancing computation (PEC) technologies are being explored as an alternative technology are data security technologies used to protect and enhance privacy and security during the collection, storage, search, and analysis of private information. PEC supports efficient, high-quality services by protecting personal data from abuse, while allowing effective use of the data, and realizing its business, scientific, and social value. PEC technologies are being explored in the following areas:

Differential privacy: Random noise is injected into the database to be mixed with personal data, while statistical estimation can still be performed using the data. This method guarantees personal privacy even when the data is shared, because the original data has been scrambled.

Homomorphic encryption: This technique allows users to perform computations on encrypted data without decrypting it. When data is homomorphically encrypted, the computations on the data are also in an encrypted form. When decrypted, the output is identical to the answers that would have been obtained if the computations had been performed on the unencrypted data.

Federated learning: This method allows data to stay in companies' local servers for machine learning. Separate learning models are built after encrypted samples have been aligned, and a virtual joint model is developed based on these models. The performance of this joint model is almost identical to a model trained on data directly gathered in the conventional way.

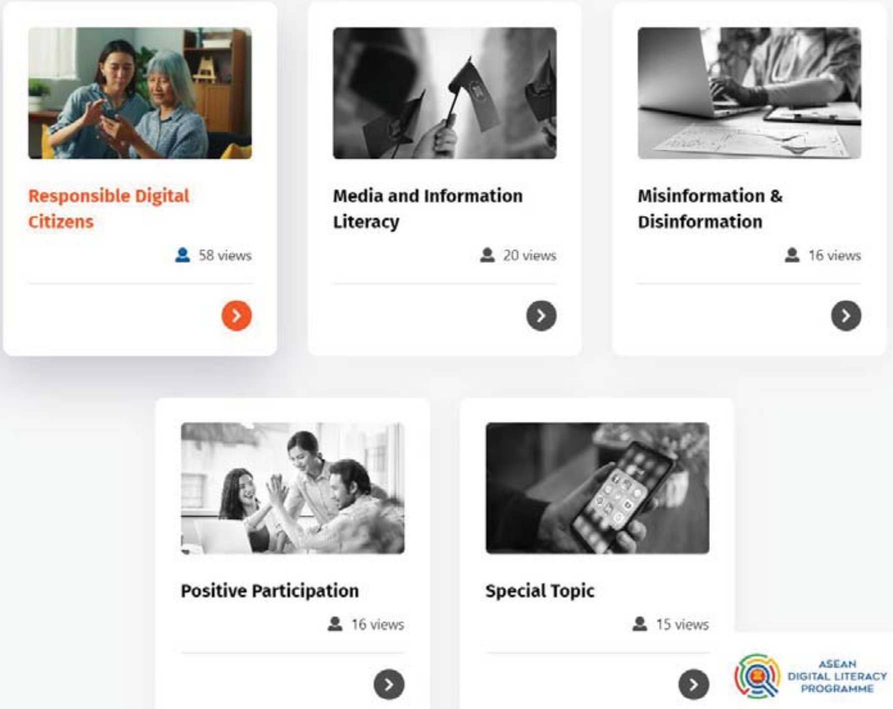
In addition to the above-mentioned technologies, PEC technologies include **a trusted execution environment (TEE), zero-knowledge proofs, k-anonymity, and l-diversity**. In the future, PEC will be supported by more algorithms and widely used in more applications, helping us to find the right balance between privacy and data value.

4. **The ASEAN Digital Innovation Programme (ADIP)**[4]
   The ASEAN Digital Innovation Programme (ADIP) is a joint initiative between the ASEAN Foundation and Microsoft that aims to create a generation of future-ready ASEAN youth. The programme serves as a platform to provide quality digital skills' training, specifically computer science education training, to underserved youth aged 15 to 35 across ASEAN blending learning approaches of in-person activities and online learning journey through Future Ready ASEAN platform (FutureReadyASEAN.org). The programme itself was officially launched on 14 March 2019 at the ASEAN Secretariat in Jakarta, Indonesia, witnessed by the Secretary-General of ASEAN Lim Jock Hoi.

   The Future Ready ASEAN platform itself was launched on May 2019, serving as a nerve centre for online training on digital skills for ASEAN youth. It can be used by trainers to curate learning journeys on computer science and digital skills, and by students for self-learning and certification. The Future Ready ASEAN platform provides four learning journeys to be able to develop capacity of young people in ASEAN, there are (a) Digital Citizen: to boost digital presence by learning how to engage in professional networks and to use web development tools; (b) Dream Team Player: to make successful team by gaining productivity, collaboration and project management skills; (c) Data Wizard: to get artificial intelligence ready by understanding, visualizing and making sense of big data sets and (d) Social Innovator: to tackle big societal challenges by learning to create technological products and applications.

5. **ASEAN Digital Literacy Programme**[5]
   Shared Target : Strengthening the Digital Literacy Skills for ASEAN Community
   The ASEAN Foundation aims to combat misinformation and disinformation by providing digital literacy training for youth, teachers, parents, community leaders and government officials.

Figure 10 Digital Class ASEAN


Responsible Digital Citizens
58 views
Media and Information Literacy
20 views
Misinformation & Disinformation
16 views
Positive Participation
16 views
Special Topic
15 views
ASEAN DIGITAL LITERACY PROGRAMME

6. **ASEAN Seeds for the Future**[6]
   ASEAN Seeds for the Future (ASEAN STF) is a programme by ASEAN Foundation in partnership with Huawei. This programme seeks to develop local ICT talent, enhance knowledge transfer, encourage a greater understanding of the ICT sector, and promote regional building and participation in the digital community.

[4] The ASEAN Digital Innovation Programme (ADIP): https://www.aseanfoundation.org/asean_digital_innovation_programme
[5] ASEAN Digital Literacy Prohramme: https://www.digitalclassasean.org/
[6] ASEAN Seeds for the Future: https://www.aseanfoundation.org/asean_seeds_for_the_future

Figure 11 ASEAN Seeds for the Future

First launched in 2008 in Thailand, the Seeds for the Future is a programme initiated by Huawei dedicated to empowering Science, Technology, Engineering, and Mathematics (STEM) and non–STEM students worldwide. The programme provides youth with the opportunity to gain work experience in Beijing and Huawei's headquarters in Shenzhen. Since the emergence of COVID-19, the Seeds for the Future has been adjusted into online immersive activities.

As the programme scales up to ASEAN level, it seeks to equip more students in the region with ICT skills to prepare them for the Industry Revolution 4.0 era. ASEAN STF seeks to address skill gaps in the region and promote inclusive education by providing youth from marginalized communities with more access to vocational training.

5.2 R-Shared Responsibilities

R-Shared Responsibilities: Only with different roles and responsibilities taken appropriately, could the ecosystem enter a 'virtuous circle' and develop rapidly.

A shared responsibility is the only path to successfully address new ICT technologies risks. The ICT industry is growing fast, highly complex, serves a wide variety of needs, and faces an increasing range of threats. The formation of an open, collaborative ecosystem for security is a necessity if the industry is to grow. Regional and national digital economy need the regulators, industries, developers, researchers, and standards organizations to work closely together, to promote commercial and technological innovation to achieve a healthy, collaborative, fast improvement of digital economy competitiveness.

The national cyber security governance maturity is a necessity to improve the competitiveness of a national digital economy. It is recommended that government cyber security regulation policies and rules take a tradeoff between economic development and cyber security regulation.

At National level:

- From economic development perspective: The national target is that the digital economy is developing rapidly, healthy, competitively and collaboratively.
- From cyber security perspective: The national cyber security maturity is a necessity to improve the competitiveness of the national 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.

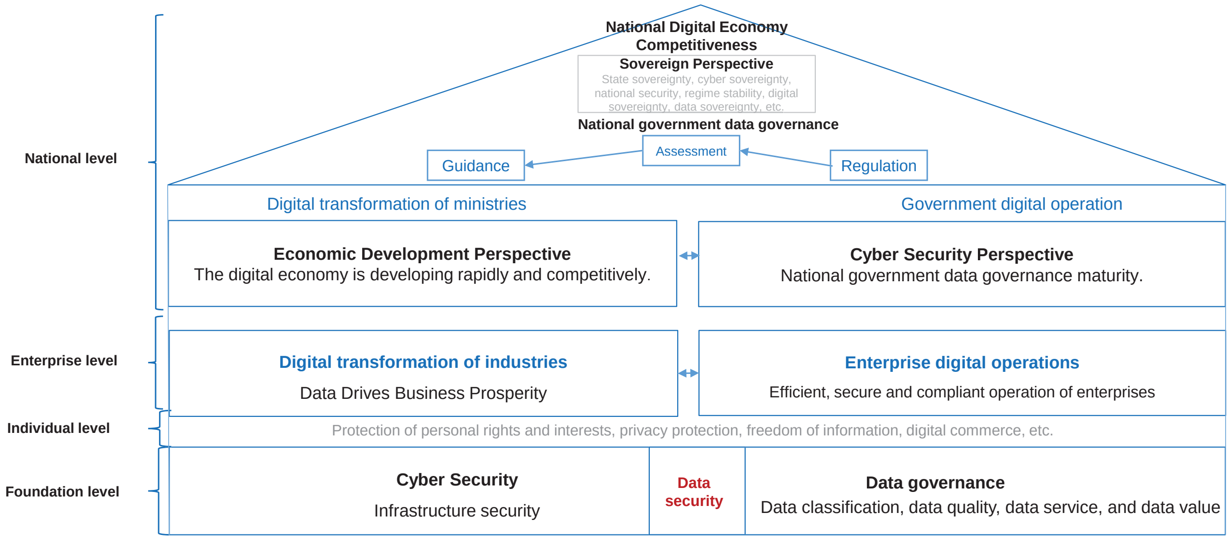
At Personal level:

- Protection of personal rights and interests, privacy protection, freedom of information, data quotient and etc. shall be considered. Data Quotient is an important measurement to measure whether modern humans have data awareness, thinking, habits, and data analysis capabilities. It measures the survival logic of the data era. This is a measurement system that reflects a person's ability to record data, organize data, maintain data, search data, analyze data, and control data.

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 12: The perspectives of economic development and cyber security


National Digital Economy Competitiveness
Sovereign Perspective
State sovereignty, cyber sovereignty, national security, regime stability, digital sovereignty, data sovereignty, etc.
National government data governance
Assessment
Guidance
Regulation
National level
Digital transformation of ministries
Government digital operation
Economic Development Perspective
The digital economy is developing rapidly and competitively.
Cyber Security Perspective
National government data governance maturity.
Enterprise level
Digital transformation of industries
Data Drives Business Prosperity
Enterprise digital operations
Efficient, secure and compliant operation of enterprises
Individual level
Protection of personal rights and interests, privacy protection, freedom of information, digital commerce, etc.
Foundation level
Cyber Security
Infrastructure security
Data security
Data governance
Data classification, data quality, data service, and data value

Which means we can understand the national data security governance from THREE perspectives as below:

- **National sovereignty**: Data is a national strategic resource like oil, soil, infrastructure, and basic production factor. A national 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.
- **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.

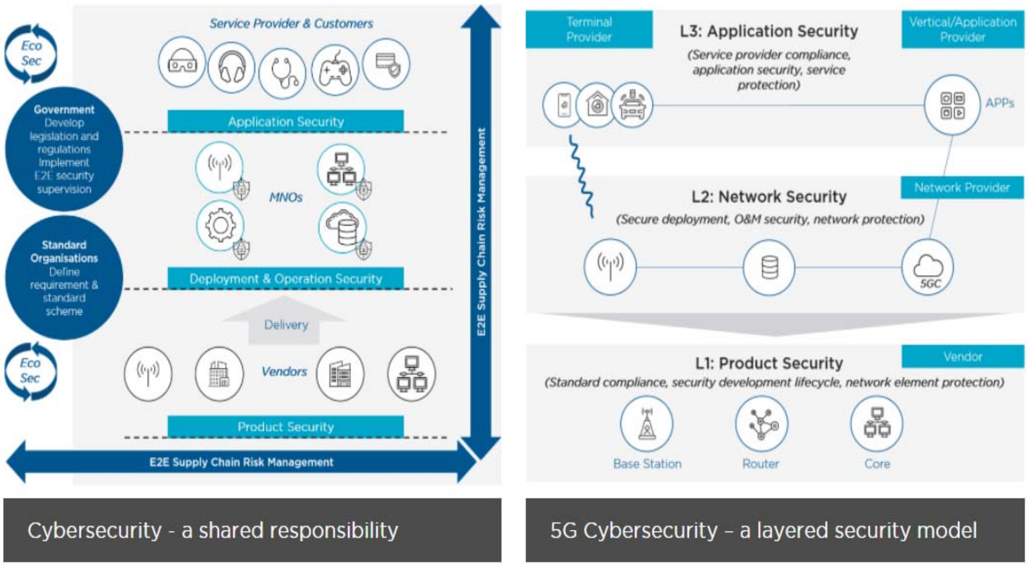
Use case:

1. **GSMA Mobile Cybersecurity Knowledge Base**[7]
   The GSMA Mobile Cybersecurity Knowledge Base (GSMA Mobile CKB) proposes that 5G cybersecurity is a shared responsibility.5G cybersecurity is a shared responsibility that involves key stakeholders including Mobile Network Operators (MNOs), interconnection providers, vendors, application developers, service providers and governments, each with a clearly defined set of responsibilities which (when fully met) can enable the deployment and operation of 5G systems in a secure manner. This means that only with appropriate different roles can responsibilities be taken in a way that the ecosystem can enter a ‘virtuous circle’ and develop rapidly.
   GSMA Mobile CKB, defining the risk mitigation responsibilities of stakeholders for each threat, released on May 30, 2021
   - Application security is the responsibility of application developers and service providers.
   - Network security is typically managed, controlled, and operated by MNOs, but some elements may also be outsourced to professional service providers.
   - Product security is the responsibility of equipment vendors, NESAS|SCAS.

   The GSMA believes that 5G security risks can be addressed through coordinated and verifiable security measures based on common standards.

[7] GSMA Mobile CKB: https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

Figure 13: GSMA Mobile Cybersecurity Knowledge Base


Eco Sec
Service Provider & Customers
Government Develop legislation and regulations Implement E2E security supervision
Application Security
MNOs
Standard Organisations Define requirement & standard scheme
Deployment & Operation Security
Delivery
Eco Sec
Vendors
Product Security
E2E Supply Chain Risk Management
E2E Supply Chain Risk Management
Cybersecurity - a shared responsibility
Terminal Provider
L3: Application Security
(Service provider compliance, application security, service protection)
Vertical/Application Provider
APPs
Network Provider
L2: Network Security
(Secure deployment, O&M security, network protection)
5GC
L1: Product Security
Vendor
(Standard compliance, security development lifecycle, network element protection)
Base Station
Router
Core
5G Cybersecurity – a layered security model

GSMA Mobile CKB serves as a practice guide for regulator and MNOs to manage 5G network security:

- End-to-end security: The Network Equipment Security Assurance Scheme (NESAS) provides security for 5G Network Element (NE) devices, and the 5G security knowledge base provides security for carrier network planning, construction, maintenance, optimization, and operation.
- Practice guide: Operators can use the 5G security knowledge base as an important reference and basis to improve 5G security assurance.
- Collaboration with all parties: Operators can cooperate with equipment vendors, application providers, and regulatory agencies to comply with security requirements set by the knowledge base.
- Security assessment: Operators can implement security control measures in the knowledge base and make assessment based on the GSMA security maturity model.

GSMA Mobile CKB is a bridge between “Operators” requirements for ensuring regulatory compliance, enhancing security/resilience, and enabling vertical industries for revenue generation” and “security capability development in 5G network planning, construction, maintenance, optimization, and operation”. Actually, the GSMA Mobile Cybersecurity Knowledge Base serves as a bridge between the requirements of operators’ supervision compliance, security resilience improvement, and enabling 5G application security and the construction of 5G network planning, maintenance, and operation security capabilities.

Meanwhile, GSMA Mobile CKB is evolving by harmonizing regulators’ requirements, technology development, and technological innovations to safeguard the interests and security of end users, enterprises, regions, and nations in 5G, 5.5G, and 6G mobile networks through a shared responsibility and a shared action.

2. OIC-CERT 5G Cyber Security Framework[8]

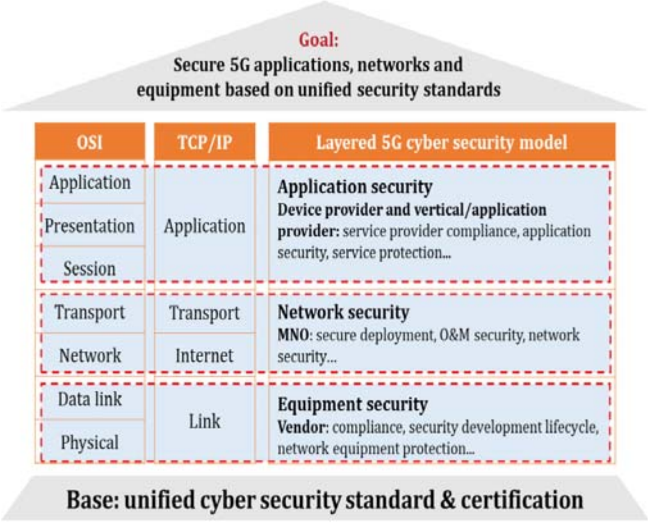
Referring to Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, the telecommunication industry has been divided into equipment, network and application layers. It is thus more practical that the OIC-CERT 5G cyber security framework focus on the security of equipment, network and application, respectively.

A layered security structure can help to clarify roles and responsibilities of implementing and deploying cyber security requirements. To ensure targeted cyber security requirements can be deployed effectively and uniformly by OIC member states, unified standards and certifications are decided as the foundation of this framework. Fragmentation and potentially conflicting cyber security requirements and compliance for OIC member states could be avoided. Besides, trust needs to be based on the truth, while truth must be verifiable, and the verification should depend on the unified

[8] OIC-CERT 5G Cyber Security Framework: https://www.oic-cert.org/en/events/5g/index.html#.YodGRKhByUk

standards. This framework does not define any standards and certification schemes, because applying or developing them depends on actual requirements for stakeholders. And there have been good standards and certifications able to be directly used.

Figure 14: OIC-CERT 5G Cyber Security Framework



Goal:
Secure 5G applications, networks and equipment based on unified security standards

OSI	TCP/IP	Layered 5G cyber security model
Application Presentation Session	Application	**Application security** **Device provider and vertical/application provider:** service provider compliance, application security, service protection...
Transport Network	Transport Internet	**Network security** **MNO:** secure deployment, O&M security, network security...
Data link Physical	Link	**Equipment security** **Vendor:** compliance, security development lifecycle, network equipment protection...

Base: unified cyber security standard & certification

A layered security approach-Roles & Responsibilities

Requirements for each layer are designed as a baseline to guide or assist OIC member states to direct and control 5G cyber security development.

It is thus easy and flexible for member states to not only understand security targets, but also combine with their realities to customize and build related 5G cyber security efficiently.

In practice, requirements are dynamic along with many aspects, such as security technologies, security mind-set and awareness, laws and regulations, current threat landscape and so on. It means that an iterative update of security requirements in different periods is essential.

- **Application Security**
  Terminal provider, Vertical/application Provider: Service Provider compliance, application security, and service protection….
  Healthcare: ISO 62304 (secure development of medical device software), ISO 14971 (risk management of medical devices), ISA / IEC 62443 EDSA - Embedded Device Security Assurance....
  Vehicles: ISO/SAE 27014…
  IoT: OWASP IoT verification standard, ETSI EN 303 645…
  ISO/IEC 27005:2018, Information security risk management
- **Network Security**
  Mobile Operator: Secure deployment, O&M security, network security…
  ISO/IEC 27001:2013 Information Security Management Systems;
  3GPP Study on security aspects of network slicing enhancement TS 33.813
  NIST cyber security framework;
  GSMA 5G Cybersecurity Knowledge Base.
- **Equipment Security**
  Vendor: compliance, security development lifecycle, and Network equipment protection …
  GSMA FS.16 Network Equipment Security Assurance Scheme-Development and Lifecycle Security Requirement v 2.0 ;
  3GPP TS 33.117 Catalogue of General Security Assurance Requirements.

A shared responsibility and collaboration

5G cybersecurity is under a shared responsibility for key stakeholders, including mobile network operators, interconnection providers, vendors, application developers, service providers, and governments.

In the OIC-CERT 5G Cyber security risk repository, it is clear that countermeasures against the same threat may involve more than one actor, which includes government and national regulators, mobile network operators, equipment vendors, and service providers.
Generally speaking, government and industry share similar goals of mitigating cybersecurity threats to network infrastructures, preventing cyberattacks, and reducing the impact of illegal cyber behaviors.

Also, public-private partnerships should be leveraged to ensure that both industry and government achieve the desired policy outcome of more secure 5G networks.

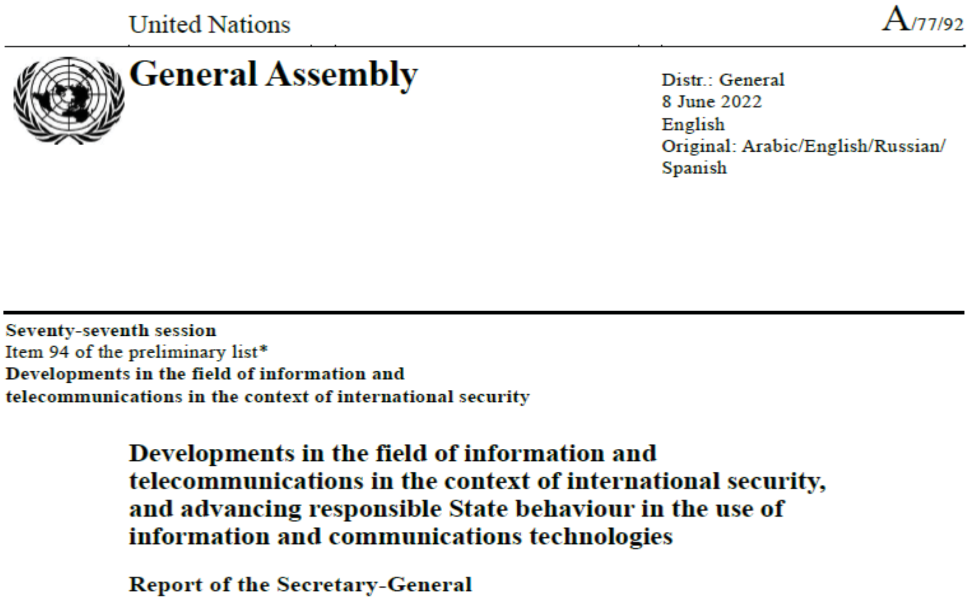
5.3 U-United Multi-stakeholders' Collaboration

U-United Multi-stakeholders' Collaboration between all stakeholders is essential.
ICT is transforming industries and governments around the world, making them digital and intelligent. Overcoming the challenges of security is part of technological advance and social progress. United Multi-stakeholders' Collaboration between all parties is vital, all stakeholders-government and industry alike-must realize that developing effective global solutions for the entire industry demands more openness, more candid engagement, and honest, open communications. Users, regulators, industry experts, governments need to leverage the collective knowledge of industry. Without this shared knowledge of the stakeholders such as the ISO/IEC, ITU, local governments, academics, ETSI, ENISA, other ICT corporations and players, innovation will be stifled within the industry and risks will not be highlighted at an early stage. We need to build security through innovation. We need to invest in researching cutting-edge security technology and use technology to meet the challenges of technology.

Use case:

1. **United Nations General Assembly A_77_92"a community of shared future for humankind"**[9]

Figure 15: United Nations General Assembly A_77_92



United Nations A/77/92

General Assembly

Distr.: General
8 June 2022
English
Original: Arabic/English/Russian/
Spanish

Seventy-seventh session
Item 94 of the preliminary list*
Developments in the field of information and
telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies

Report of the Secretary-General

UNITED NATIONS, Nov. 4 2022--The United Nations General Assembly First Committee has included in its three resolutions the notion of "a community of shared future for humankind". In the voting, the inclusion of the notion was supported by more than 100-member states on all occasions. The shared vision is "A community of shared future for humankind in cyber space is an indispensable part of a global village of shared future" and "Achieving shared development, ensuring common security, realizing joint governance, and enjoying benefits together".

2. **First Global AI Statement**[10]
The Bletchley Declaration, First Global AI Statement, China, EU and relevant 28 countries signed at the AI Safety Summit, 1-2 November 2023.

[9] United Nations General Assembly A_77_92: https://digitallibrary.un.org
[10] Policy paper The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

Figure 16: The Bletchley Declaration: Shaping the Future of AI Together[11]

“In the context of our cooperation, and to inform action at the national and international levels, our agenda for addressing frontier AI risk will focus on:

Identifying AI safety risks of shared concern, building a shared scientific and evidence-based understanding of these risks, and sustaining that understanding as capabilities continue to increase, in the context of a wider global approach to understanding the impact of AI in our societies.

building respective risk-based policies across our countries to ensure safety in light of such risks, collaborating as appropriate while recognizing our approaches may differ based on national circumstances and applicable legal frameworks. This includes, alongside increased transparency by private actors developing frontier AI capabilities, appropriate evaluation metrics, tools for safety testing, and developing relevant public sector capability and scientific research.”

United Multi-stakeholders’ Collaboration on global AI governance, Human-centric, Trustworthy, Responsible, Collaboration are shared target and shared action.

3. RCEP Innovation and Digital Ecosystem MADANI (RIDE MADANI)[12]

Figure 17: RIDE MADANI

[11] The Bletchley Declaration: Shaping the Future of AI Together: https://opengovasia.com/the-bletchley-declaration-shaping-the-future-of-ai-together/

[12] RIDE MADANI: https://www.thestar.com.my/business/business-news/2023/11/21/mcdc-launches-ride-madani-initiative-attracts-rm100bil-in-investments

RIDE MADANI announced “**Three 100s**” initiative, which includes proposing that 100 enterprises jointly initiate the Ride Madani Alliance, investing RM100 billion in Malaysia over the next five years, and nurturing at least 100 young leaders each year.

RIDE MADANI will jointly build the RCEP Innovation and Digital Ecology Demonstration Zone in Kuala Lumpur, Malaysia, including AI Computing Data Center, Regional Headquarters for Investment in Green Energy, Asia Headquarters for 5G Infrastructure and Application Services, Regional Headquarters for Digital Marketing, and Training Center. In this way, Kuala Lumpur, Malaysia, will become the headquarters of the MADANI and the beacon of the digital economy in the RCEP region.

Deputy Prime Minister Datuk Seri Fadillah Yusof highlighted the significance of digitalization and sustainability in driving Malaysia’s economic growth and resilience.

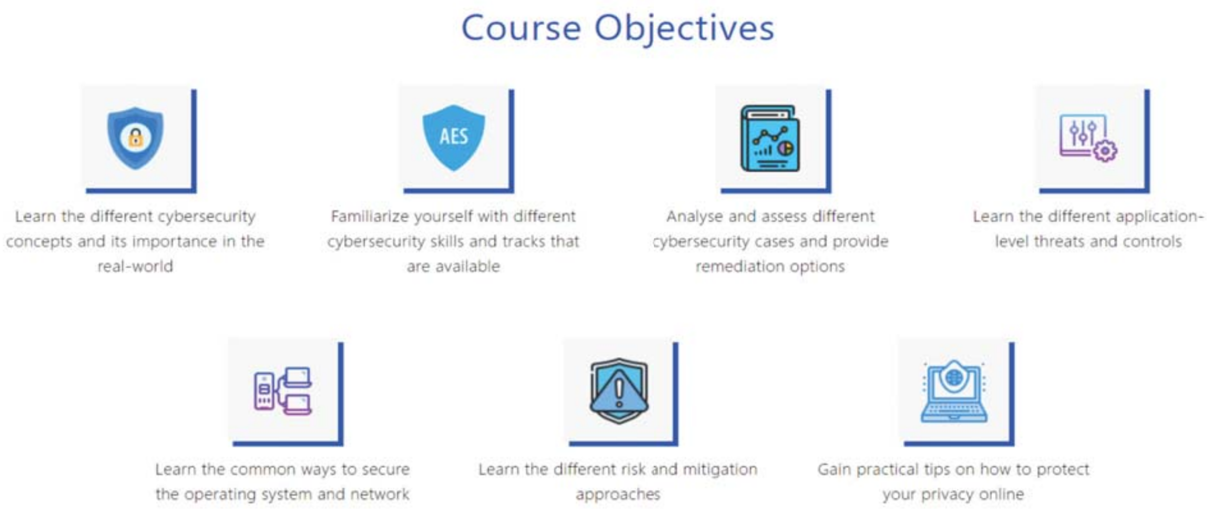
4. **ASEAN Cybersecurity Skilling Programme (ASEAN CSP)**[13]

The ASEAN Foundation and Microsoft are proud to announce the successful completion and impact of ASEAN Cybersecurity Skilling Programme (ASEAN CSP).

First launched in January 2022, ASEAN CSP was delivered by ASEAN Foundation with support from Microsoft to raise awareness on the danger of cyber threats and bring attention to the importance of equipping the people of ASEAN, especially those from marginalised community, with adequate knowledge about cybersecurity to fight against the ever-growing cybercrimes.

This initiative was built upon Microsoft’s expertise and commitment in promoting a safer digital space and the ASEAN Foundation’s long track record of catalysing educational growth in the region. Over the span of 15 months, ASEAN CSP has managed to deliver cybersecurity training covering cybersecurity awareness fundamentals to over 24,000 beneficiaries in Indonesia, Malaysia, Thailand, the Philippines, Vietnam, Singapore, and Cambodia in collaboration with 634 master trainers and 10 local implementing partners.

Figure 18: ASEAN Cybersecurity Skilling Programme



Course Objectives

Learn the different cybersecurity concepts and its importance in the real-world

Familiarize yourself with different cybersecurity skills and tracks that are available

Analyse and assess different cybersecurity cases and provide remediation options

Learn the different application-level threats and controls

Learn the common ways to secure the operating system and network

Learn the different risk and mitigation approaches

Gain practical tips on how to protect your privacy online

This regional initiative will empower educators, non-profit trainers, government officials and youth across ASEAN through training to prepare them to deliver cybersecurity knowledge and information to 30,000 end beneficiaries across ASEAN. This programme will also create an inclusive platform in different ASEAN languages to further promote cybersecurity awareness and provide accessible e-learning platform.

ASEAN CSP is set to implement the following key activities:

1) Baseline Survey: The programme will conduct a survey and a series of FGD (Focus Group Discussion) and roundtable discussions on issues around cybersecurity to raise awareness and identify best practices to prevent and respond to online threats.

[13] ASEAN Cybersecurity Skilling Programme: https://www.aseanfoundation.org/asean_cybersecurity_skilling_programme

2) Training of Trainer (ToT) on Cybersecurity Workshops: A total of 14 Training of Trainers workshops will be organized for 560 trainers across ASEAN using the toolkit/module supported by Microsoft and other trusted sources.
3) Localized Cybersecurity Courses for Local Communities: Trainers who have joined the Training of Trainer Workshop will be encouraged to deliver a workshop online/offline at the local level.

5. Uniting for an Inclusive Digital Future[14]

In a collective move to fortify the digital skills pipeline, Huawei, the ASEAN Foundation, and the Southeast Asia Ministers of Education Organization (SEAMEO) hosted the Seeds for the Future Summit 2023 at Shanghai, on September 19, 2023. Under the theme "Connect, Cultivate, Contribute for Inclusive Digital Talent Growth in Asia-Pacific," the summit convened 91 exceptional participants of Seeds for the Future, Huawei's flagship talent initiative, from 19 Asia-Pacific countries, emphasizing the vital role of youth in the digital evolution of the region.

Figure 19: Officials and representatives from ASEAN and international organizations
celebrating the regional digital talent growth together with 91 students from 19 Asia-Pacific countries

Officially opening the event, H.E. Dr. Kao Kim Hourn, Secretary-General of ASEAN, remarked, "I strongly encourage private-led initiatives that share the vision for attracting and nurturing digital talents such as the Seeds for the Future programme. I hope it will provide more opportunities for the youth, as well as pay special consideration for the vulnerable groups such as women, people with disabilities, and those from rural areas to ensure balanced participation and inclusivity."

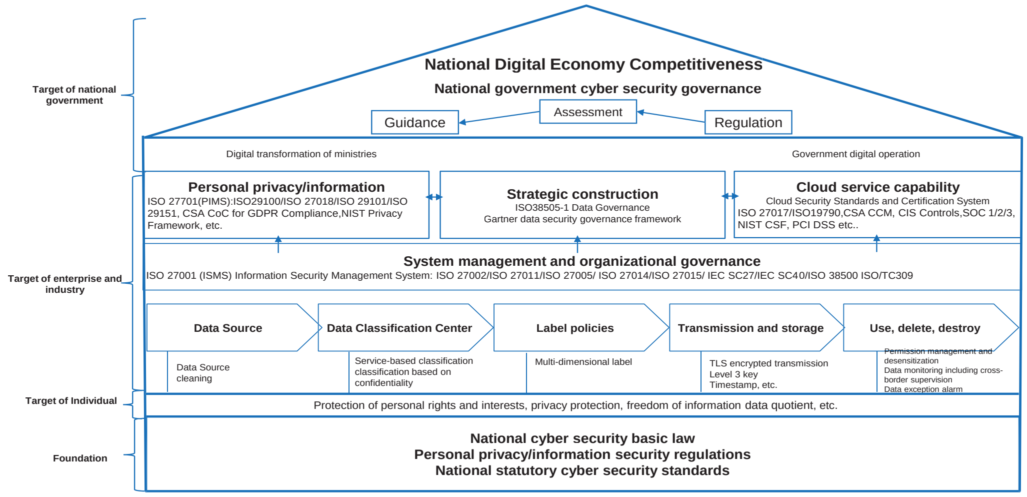
As a pivotal of the summit, Huawei and the International Telecommunications Union (ITU) announced a joint declaration focusing on **six key areas** of digital collaboration across the Asia-Pacific, including ICT policy and regulation, joint research, inclusive infrastructure, digital capacity-building, girls and youth empowerment, and digital practice-sharing.

5.4 S-International Common Standardization

S-Standardized Baseline and International Common Standard to follow: As the global market grows, a standardized baseline for both ICT development and cybersecurity together is essential to avoid fragmentation. This is also demonstrated by developing standards for cybersecurity by aligning standards similar to the CAR 2 CAR Communication Consortium(C2C-CC) and World Wide Web Consortium (W3C) consortia that have guided the development of the world wide web making it accessible to all. We call on the entire ICT industry to invest more resources in creating comprehensive security and quality systems for communications networks, and reliable standards against which to assess them. We believe that the industry should develop globally-accepted, government & industry-led, voluntary 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, for example governments take the lead in establishing national data security governance framework system by international common standards in line with domestic situation as below:

[14] Uniting for an Inclusive Digital Future:
https://www.apac-business.com/companies/corp-events/uniting-for-an-inclusive-digital-future-huawei-asean-foundation-and-seameo-empower-asia-pacifics-young-tech-talents/

Figure 20: National Data Security Governance Framework[15]


Target of national government
Target of enterprise and industry
Target of Individual
Foundation
National Digital Economy Competitiveness
National government cyber security governance
Guidance
Assessment
Regulation
Digital transformation of ministries
Government digital operation
Personal privacy/information
ISO 27701(PIMS):ISO29100/ISO 27018/ISO 29101/ISO 29151, CSA CoC for GDPR Compliance,NIST Privacy Framework, etc.
Strategic construction
ISO38505-1 Data Governance
Gartner data security governance framework
Cloud service capability
Cloud Security Standards and Certification System
ISO 27017/ISO19790,CSA CCM, CIS Controls,SOC 1/2/3, NIST CSF, PCI DSS etc..
System management and organizational governance
ISO 27001 (ISMS) Information Security Management System: ISO 27002/ISO 27011/ISO 27005/ ISO 27014/ISO 27015/ IEC SC27/IEC SC40/ISO 38500 ISO/TC309
Data Source
Data Classification Center
Label policies
Transmission and storage
Use, delete, destroy
Data Source cleaning
Service-based classification classification based on confidentiality
Multi-dimensional label
TLS encrypted transmission
Level 3 key
Timestamp, etc.
Permission management and desensitization
Data monitoring including cross-border supervision
Data exception alarm
Protection of personal rights and interests, privacy protection, freedom of information data quotient, etc.
National cyber security basic law
Personal privacy/information security regulations
National statutory cyber security standards

National data security governance framework references are 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.

These standards can be used as national data security governance framework to standardize cloud service provider (CSPs) and cloud service customer (CSCs) 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 in collaboration to develop more secure cloud service as a key guideline.

Use case:

1. **UN :A multi-stakeholder High-Level Advisory Body for Artificial Intelligence reported on global AI governance around the end of 2023**[16]

   Secretary-General António Guterres Convenes Critical Body to Debate Global Governance of Artificial Intelligence.

   Such an entity could gather knowledge and expertise and put it at the disposal of Member States and the international community. It could support collaboration on the research of AI tools to accelerate sustainable development.

   As a first step, the Secretary-General is convening a multi-stakeholder High-Level Advisory Body for Artificial Intelligence that will report back for options for global AI governance by the end of the year. This is a unique opportunity for experts from governments, private sector, civil society, the technology sector, and academia to come together to create a global scientific consensus on opportunities and risks of AI, and provide guidance to the international community on how best to govern AI in the benefit of all humanity.

   Already some elements of this governance framework are emerging around data protection, risk-based assessments of AI algorithms and the responsible use of AI systems. Data must be accurate, representative and gathered justly. Algorithms must be tested for safety and must not discriminate. AI must be used for good and not subverted for nefarious goals.

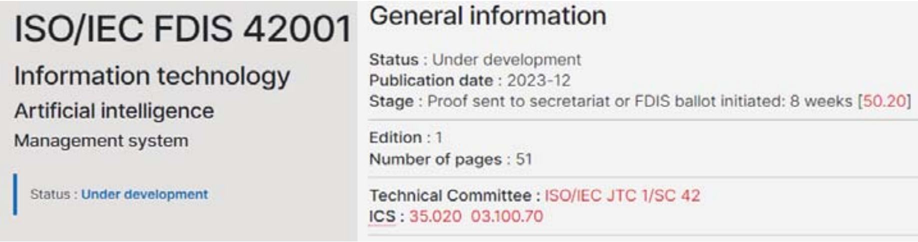
[16] UN:A multi-stakeholder High-Level Advisory Body for Artificial Intelligence will report on global AI governance by the end of 2023
https://unu.edu/article/secretary-general-antonio-guterres-convenes-critical-body-debate-global-governance

Powerful technologies like AI have a Janus-like character. Like the two-faced Roman god, they herald a transition from the past to something new. Who steers these transitions and for what purpose is a critical public policy question.

We must debate the changes that AI will herald in the inclusive multilateral setting of the United Nations. The Secretary-General's multistakeholder Advisory Body on AI is the right starting point for this global conversation.

2. **ISO/IEC FDIS 42001 Information technology Artificial intelligence Management system (ISO/IEC JTC 1/SC 42)**[17]

Figure 21: ISO/IEC FDIS 42001



ISO/IEC FDIS 42001

Information technology

Artificial intelligence

Management system

Status : Under development

General information

Status : Under development
Publication date : 2023-12
Stage : Proof sent to secretariat or FDIS ballot initiated: 8 weeks [50.20]

Edition : 1
Number of pages : 51

Technical Committee : ISO/IEC JTC 1/SC 42
ICS : 35.020 03.100.70

3. **ISO/IEC 38507:2022 governance implications of the use of AI**[18]

ISO/IEC 38507 provides guidance for members of the governing body of an organization to enable and govern the use of Artificial Intelligence (AI), in order to ensure its effective, efficient and acceptable use within the organization.

- ISO/IEC 38507 document also provides 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;
- public authorities and policymakers;
- internal and external service providers (including consultants);
  assessors and auditors.

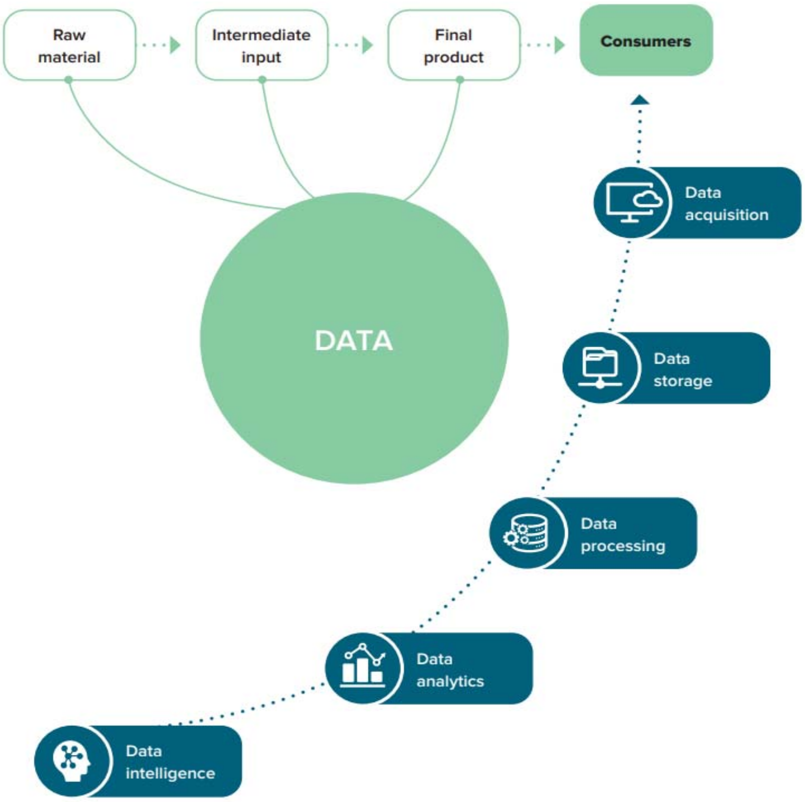
ISO/IEC 38507 document is applicable to the governance of current and future uses of AI as well as the implications of such use for the organization itself.
ISO/IEC 38507document is applicable to any organization, including public and private companies, government entities and not-for-profit organizations. This document is applicable to an organization of any size irrespective of their dependence on data or information technologies.

5.5 T-Fair Digital Trade

Digital trade goes beyond trade in services as it includes goods that are wholly or partially ordered or delivered through digital means. Definitions of digital trade vary, but the concept usually includes ICT goods and digital-based services. E-commerce, is usually defined to encompass the delivery of goods ordered online, is part of the larger category of digital trade. Digital trade in services – including financial services; telecommunications, computer and information services; business services; audio-visual and recreational services-has been growing rapidly, driving much of the increase in global services trade. Because digital trade spans both goods and services, it faces a broader range of potential barriers than trade in goods. Digital trade in services is affected by policy measures that apply at the border and by regulation that applies behind the border. Restrictive national regulation may have negative consequences for trade and the ability of firms to connect and use digital platforms to provide services to both local customers and foreign clients. The impact of foreign regulatory regimes that impede or simply exclude domestic firms from engaging in cross-border digital transactions is important from a digital transformation perspective. A broader data and digital regulation are particularly important for firms that rely on data as a core part of their business, such as platform companies and providers of "software as a service" and "data as a service".

[17] ISO/IEC FDIS 42001 Information technology Artificial intelligence Management system (ISO/IEC JTC 1/SC 42): https://www.iso.org/standard/81230.html
[18] ISO/IEC 38507:2022 governance implications of the use of AI, https://www.iso.org/standard/56641.html

Figure 22. Value chains in the digital economy[19]



The ultimate purpose of cyber security governance is to create value by improvement of the efficiency, interoperability and reliability of digital trade.

>60 countries have signed Digital Economy Agreements between regions and nations such as ASEAN-China Free trade agreement(FTA)[20] signed on November 2002 is on upgrading to FTA 3.0, Digital Economy Partnership Agreement (DEPA)[21] signed on 12th Jun. 2020, Framework for Negotiating ASEAN Digital Economy Framework Agreement (DEFA)[22] on 6th Sep. 2023 and Initiative on International Trade and Economic Cooperation Framework for Digital Economy and Green Development[23] on 18th Oct.2023. And current typical modules of Digital Economy Agreements (DEAs) are as below:

Figure 23: Current Typical Modules of DEAs (Digital Economy Agreements)

- **Artificial Intelligence**

The DEAs promote the adoption of ethical AI governance frameworks, which set out principles to harness AI responsibly. This would help create consensus on governance and ethics principles and build trust in AI systems used across borders.

- **Data Innovation**

With DEAs, organizations can receive better support to develop new products and services as Governments promote data-driven innovation across borders.

- **Digital IDs**

Digital IDs provide data from government-verified sources to form a digital user profile. Among other benefits, digital IDs significantly streamline business processes, including company registrations and opening of corporate bank accounts.

- **Cross-border data flows**

Cross-border data flows are increasingly important to the growth of the digital economy as it supports electronic commerce and other digitally-enabled activities, such as data analytics and AI. Under the DEAs, parties agree to allow data to flow freely across borders and prohibit the localization of data except for legitimate purposes such as personal data protection.

- **Personal data protection**

The protection of personal data is key to maintaining trust in the digital economy and the development of cross-border trade.

- **Fintech, E-payments and E-invoicing**

FinTech, is an economic industry composed of companies that use technology to make financial services more efficient.
E-payments provide a convenient alternative to cash and cheques as payment modes.
E-invoicing is the automated creation, exchange and processing of requests for payment between suppliers and buyers using a structured digital format.

- **Open Government Information**

Expand access to and use of open government data to generate new opportunities for business, especially SMEs

- **Digital Trade Standards System**

Improvement of the efficiency, interoperability, and reliability of digital trade.

- **Reliable data transaction**

Data monetization and relevant data evaluation standards and certification services.

- **SMEs Go Digital**

Small and medium enterprises (SMEs) are an indispensable part of the healthy development of digital economy.

……

[19] Digital Trade Opportunities and Challenges, https://www.wto.org/english/tratop_e/devel_e/digital_trade2022_e.pdf
[20] ASEAN-China FTA, https://fta.miti.gov.my/index.php/pages/view/asean-china?mid=33
[21] Digital Economy Partnership Agreement (DEPA), https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement
[22] Framework for Negotiating ASEAN Digital Economy Framework Agreement, https://asean.org/wp-content/uploads/2023/09/Framework-for-Negotiating-DEFA_ENDORSED_23rd-AECC-for-uploading.pdf
[23] Initiative on International Trade and Economic Cooperation Framework for Digital Economy and Green Development, https://www.mfa.gov.cn/eng/zxxx_662805/202310/P020231020384764366957.pdf

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 23: Digital Trade Standards Systems Framework[24]

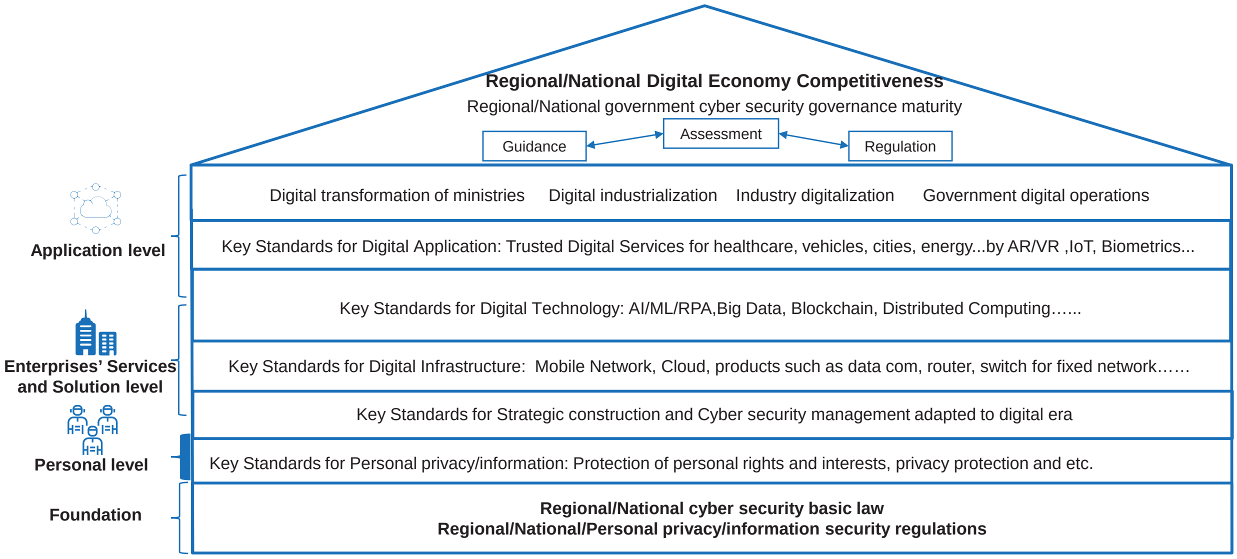

Regional/National Digital Economy Competitiveness
Regional/National government cyber security governance maturity
Guidance
Assessment
Regulation
Application level
Digital transformation of ministries
Digital industrialization
Industry digitalization
Government digital operations
Key Standards for Digital Application: Trusted Digital Services for healthcare, vehicles, cities, energy...by AR/VR ,IoT, Biometrics...
Enterprises' Services and Solution level
Key Standards for Digital Technology: AI/ML/RPA,Big Data, Blockchain, Distributed Computing……
Key Standards for Digital Infrastructure: Mobile Network, Cloud, products such as data com, router, switch for fixed network……
Key Standards for Strategic construction and Cyber security management adapted to digital era
Personal level
Key Standards for Personal privacy/information: Protection of personal rights and interests, privacy protection and etc.
Foundation
Regional/National cyber security basic law
Regional/National/Personal privacy/information security regulations

Table 1: Digital Trade Standards Systems Series

1.	**Key Standards for Digital Application**	**AR/VR**	ISO/IEC 18038:2020 Information technology — Computer graphics, image processing and environmental representation— Sensor representation in mixed and augmented reality[25]
			ISO/IEC 18039:2019 Information technology — Computer graphics, image processing and environmental data representation — Mixed and augmented reality (MAR) reference model[26]
			IEEE P2048 Standard for Augmented Reality on Mobile Devices: General Requirements for Software Framework, Components, and Integration[27]
			IEEE P3141 Standard for 3D Body Processing[28]
		IoT	ISO/IEC 21823-1:2019 Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework[29]
			ISO/IEC 21823-2:2020 Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability[30]
			ISO/IEC 21823-3:2021 Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability[31]
			ISO/IEC 21823-4:2022 Internet of things (IoT) — Interoperability for IoT systems — Part 4: Syntactic interoperability[32]
			ETSI SR 003 680 Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach[33]

[24] Malaysia Data Security Governance Reference Book: https://pikom.org.my/2023/DSG/Malaysia_Data_Security_Governance_Reference_Book.pdf

[25] 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

[26] 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

[27] 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/

[28] IEEE P3141 Standard for 3D Body Processing, https://standards.ieee.org/ieee/3141/10825/

[29] ISO/IEC 21823-1:2019 Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework, https://www.iso.org/standard/71885.html

[30] ISO/IEC 21823-2:2020 Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability, https://www.iso.org/standard/80986.html

[31] ISO/IEC 21823-3:2021 Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability, https://www.iso.org/standard/83752.html

[32] ISO/IEC 21823-4:2022 Internet of things (IoT) — Interoperability for IoT systems — Part 4: Syntactic interoperability, https://www.iso.org/standard/84773.html

[33] 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

			ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements[34]
			OWASP IoT verification standard[35]
		Biometrics	ISO/IEC JTC 1/SC 37 Biometrics[36]
		Healthcare	ISO 62304 Medical device software — Software life cycle processes[37]
			ISO 14971 Medical devices — Application of risk management to medical devices[38]
2	**Key Standards for Digital Technology**	**AI/ML/RPA**	ISO/IEC FDIS 42001 Information technology Artificial intelligence Management system
			ISO/IEC 38507:2022 governance implications of the use of AI
			ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence[39]
		Big Data	ISO/IEC 20546:2019 Information Technology-Big Data-Overview and vocabulary[40]
			ISO/IEC TR 20547:2020 Information Technology-Big data reference architecture[41]
			IEEE BDGMM BIG DATA GOVERNANCE AND METADATA MANAGEMENT: STANDARDS ROADMAP[42]
		Blockchain	ITU-T SG16 Q22 Multimedia aspects of distributed ledger technologies and e-services[43]
			TC590 National Technical Committee for Standardization of Blockchain and Distributed Accounting Technology[44]
		Distributed Computing	ISO/IEC TR 23188:2020 Information Technology-Cloud computing-Edge computing landscape[45]
			ISO/IEC JTC 1/SC 38 (Series) Cloud computing and distributed platforms[46]
3	**Key Standards for Digital Infrastructure**	**Mobile Network**	3GPP Release15/16/17/18[47]
			3GPP Study on security aspects of network slicing enhancement TS 33.813[48]
			GSMA Mobile CKB
		Wireless equipment	ITU-T work programme SG17 X.5G sec-guide[49]
			NESAS|SCAS [50]
		Cloud service	ISO/IEC 27017:2015 Information Technology-Security Techniques-Code of practice for information security controls based on ISO/IEC 27002 for cloud services [51]
			ISO/IEC 19790:2012 Information Technology-Security Techniques-Security requirements for cryptographic modules [52]
			ISO/IEC 27034-1:2011 Information Technology-Security Techniques-Application security — Part 1: Overview and concepts [53]
			Cloud Controls Matrix (CCM) [54]
			CIS Critical Security Controls Version 8[55]

[34] 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
[35] OWASP IoT verification standard, https://owasp.org/www-project-iot-security-verification-standard/
[36] ISO/IEC JTC 1/SC 37 Biometrics, https://www.iso.org/committee/313770.html
[37] ISO 62304 Medical device software — Software life cycle processes, https://www.iso.org/standard/38421.html
[38] ISO 14971 Medical devices — Application of risk management to medical devices, https://www.iso.org/standard/72704.html
[39] ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence, https://www.iso.org/standard/77608.html
[40] ISO/IEC 20546:2019 Information Technology-Big Data-Overview and vocabulary, https://www.iso.org/standard/77608.html
[41] ISO/IEC TR 20547:2020 Information Technology-Big data reference architecture, https://www.iso.org/standard/71275.html
[42] 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
[43] 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
[44] TC590 National Technical Committee for Standardization of Blockchain and Distributed Accounting Technology, https://std.samr.gov.cn/search/orgDetailView?tcCode=TC590
[45] ISO/IEC TR 23188:2020 Information Technology-Cloud computing-Edge computing landscape, https://www.iso.org/standard/74846.html
[46] ISO/IEC JTC 1/SC 38 (Series) Cloud computing and distributed platforms, https://www.iso.org/committee/601355.html
[47] 3GPP Release15/16/17/18, https://www.3gpp.org/specifications-technologies/releases
[48] 3GPP Study on security aspects of network slicing enhancement TS 33.813, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3541
[49] ITU-T work programme SG17 X.5G sec-guide, https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15006
[50] NESAS|SCAS, https://www.gsma.com/security/network-equipment-security-assurance-scheme/
[51] 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
[52] ISO/IEC 19790:2012 Information technology-Security techniques-Security requirements for cryptographic modules, https://www.iso.org/standard/52906.html
[53] ISO/IEC 27034-1:2011 Information technology-Security techniques-Application security — Part 1: Overview and concepts, https://www.iso.org/standard/44378.html
[54] Cloud Controls Matrix (CCM), https://cloudsecurityalliance.org/research/cloud-controls-matrix/
[55] CIS Critical Security Controls Version 8, https://www.cisecurity.org/controls/v8

			SOC 1/2/3[56]
		Fixed network	The Common Criteria[57]
4	**Key Standards of Strategic Construction**	**Organization**	ISO38505-1 Data Governance[58]
5	**Key Standards for Personal privacy/information: Protection of personal rights and interests,privacy protection and etc**		ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection- Information security management systems-Requirements [59]
			ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls [60]
			ISO/IEC 27011:2016 Information Technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations [61]
			ISO/IEC 27005:2018 Information Technology-Security techniques -Information security risk management [62]
			ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security[63]
			COBIT[64]
			ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection [65]
			ISO/IEC JTC 1/SC 40 IT service management and IT governance [66]
			ISO/IEC 38500:2015 Information technology — Governance of IT for the organization [67]
			ISO/TC 309 Governance of organizations[68]
			ISO/IEC 27701:2019(en) Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines [69]
			ISO/IEC 29100:2011 Information Technology-Security Techniques-Privacy framework [70]
			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 [71]
			ISO/IEC 29101:2018 Information Technology-Security Techniques-Privacy architecture framework[72]
			ISO/IEC 29151:2017 Information Technology-Security Techniques-Code of practice for personally identifiable information protection,2017[73]
			CSA CoC for GDPR Compliance[74]

[56] SOC 1/2/3, https://www.aicpa.org/cpe-learning/course/soc--for-cybersecurity-certificate-program
[57] The Common Criteria, https://www.iso.org/standard/56639.html
[58] ISO38505-1 Data Governance, https://www.iso.org/standard/56639.html
[59] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection- Information security management systems-Requirements, https://www.iso.org/standard/82875.html
[60] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, https://www.iso.org/standard/75652.html
[61] 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
[62] ISO/IEC 27005:2018 Information Technology-Security techniques -Information security risk management, https://www.iso.org/standard/75281.html
[63] ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security, https://www.iso.org/standard/74046.html
[64] COBIT, https://www.isaca.org/resources/cobit
[65] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, https://www.iso.org/committee/45306.html
[66] ISO/IEC JTC 1/SC 40 IT service management and IT governance, https://www.iso.org/committee/5013818.html
[67] ISO/IEC 38500:2015 Information technology — Governance of IT for the organization, https://www.iso.org/standard/62816.html
[68] ISO/TC 309 Governance of organizations, https://www.iso.org/committee/6266703.html
[69] 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
[70] ISO/IEC 29100:2011 Information Technology-Security Techniques-Privacy framework, https://www.iso.org/standard/45123.html
[71] 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
[72] ISO/IEC 29101:2018 Information Technology-Security Techniques-Privacy architecture framework, https://www.iso.org/standard/75293.html
[73] ISO/IEC 29151:2017 Information Technology-Security Techniques-Code of practice for personally identifiable information protection, https://www.iso.org/standard/62726.html
[74] CSA CoC for GDPR Compliance, https://cloudsecurityalliance.org/privacy/gdpr/code-of-conduct/

Use case:

1. United Nations Commission on International Trade Law[75]

In an increasingly economically interdependent world, the importance of developing and maintaining a robust cross-border legal framework for the facilitation of international trade and investment is widely acknowledged. The United Nations Commission on International Trade Law (UNCITRAL) plays a key role in developing that framework in pursuit of its mandate to further the progressive harmonization and modernization of the law of international trade. UNCITRAL does this by preparing and promoting the use and adoption of legislative and non-legislative instruments in a number of key areas of commercial law.

UNCITRAL texts are developed through an international process involving a variety of participants. UNCITRAL membership is structured so as to be representative of different legal traditions and levels of economic development, and its procedures and working methods ensure that UNCITRAL texts are widely accepted as offering solutions appropriate to many countries at different stages of economic development.

To implement its mandate and to facilitate the exchange of ideas and information, UNCITRAL maintains close links with international and regional organizations, both inter-governmental and non-governmental, that are active participants in the work programme of UNCITRAL and in the field of international trade and commercial law.

2. ASEAN Digital Economy Framework Agreement (DEFA)[20]

ASEAN DEFA negotiations will consider including but not be limited to the following elements:

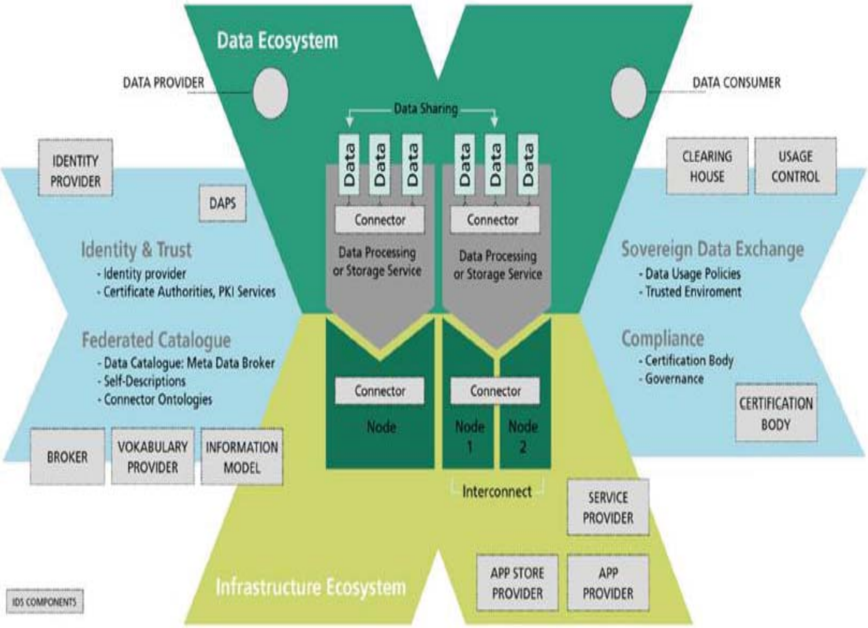
1) Digital Trade aims to facilitate cross-border trade by creating a seamless trade experience with electronic documents and interoperable processes.
2) Cross-border E-Commerce aims to create a more efficient and fairer environment for cross-border e-commerce, including digital goods and services.
3) Payments and E-Invoicing aims to promote digital payments and electronic invoicing by fostering technical interoperability, encourage innovation and competition, and developing relevant regulation.
4) Digital ID and Authentication aims to develop a mutual recognizable and interoperable digital identity and electronic authentication framework within the region.
5) Online Safety and Cybersecurity aim to improve cooperation in cybersecurity and create an open and secure online environment, with comprehensive protection to parties in a digital transaction.
6) Cross-border Data Flows and Data Protection aims to facilitate cross-border data flow and establish frameworks to protect data privacy.
7) Competition Policy aims to create a fair/non-discriminatory, transparent competitive environment with consistent guidelines on enforcement and better choice for consumers
8) Cooperation on Emerging Topics aims to establish mechanisms for regulatory cooperation for relevant standards and regulations to keep up with technological innovations in emerging topics such as AI.
9) Talent Mobility and Cooperation aims to facilitate digital talent mobility between countries and close collaboration on talent building.

3. Creating business value through data services based on the data sovereignty cloud and IDS rules

The combined architecture of GAIA-X and IDS[76] 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.

[75] United Nations Commission on International Trade Law, https://uncitral.un.org/en
[76] GAIA-X and IDS, https://internationaldataspaces.org/publications/most-important-documents/

Figure 25: Mapping of IDS Components into the GAIA-X Architecture



Digital Trust is much more than just a value, it is an ecosystem.

Digital trust cannot be an assumption of shared values and behavior but needs to be a tangible process that reflects the diverse expertise and voices of all stakeholders. Only in this way will standards be agreed and implemented.

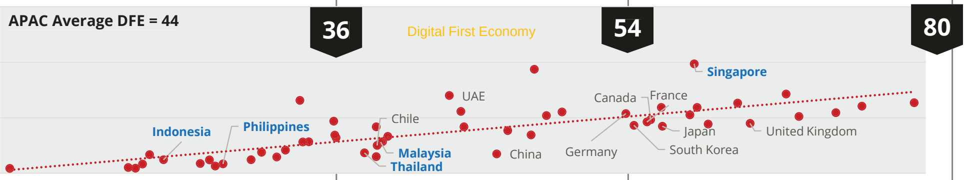
With 5G/6G, AI/Gen AI, Cloud facilitating more data exchange and opportunities it is essential that we are able to enjoy the benefits in a secure, sustainable way that protects all assets from the dangers of cyber-attacks.

According to the UN’s Secretary-General’ s Roadmap for Digital Cooperation by 2030, every person should have safe and affordable access to the internet. Keeping society safe whether in the delivery of education, manufacturing or food delivery is essential. Connectivity is a right and all users in society deserve to be safe - whether corporations, governments or individuals and more importantly is the life quality in the intelligent world 2030 safeguarded by Digital Trust Model.

6 Way Forward : DATA+AI+Green

We call on a community of shared future for humankind in cyberspace is an indispensable part of a global village of shared future. Embracing the DATA+AI+Green era and achieving shared development and benefits together in line with the local domestic situation as below:

Figure 26: One country, one strategy for digital economy development

DFE index developed to enable continuous measurement of development progress			
Adopter Highest scores in Policy and Connectivity	**Accelerator** Joint high score in Policy and Connectivity Quality/ Cloud	**Advanced** Policy, Investment, Connectivity Quality/ Cloud/ Data AI highest	Aspiration
			Achieving an Intelligent World 2030, **Data + AI + Green**
• Building nationwide digital connectivity • Digital growth mainly from communication, eCommerce and services upon networks • Accelerating improvement of cyber security governance maturity • AI Proof of concept (POC) for Ministries & Industries	• Increasing ICT investments and talent development • Building highspeed digital connectivity to drive cloud computing for Gov. and Industries • Improve cyber security governance maturity • Unleashing the value of reliable data • AI Innovation & Development Security & Trustworthy	• Accelerating digital transformation, data assets and monetization • Gigabit connectivity, Cloud-first environment with ICT and talent investments as primary national objectives • Achieving shared development, ensuring common security, realizing joint governance, and enjoying benefits together • GenAI goto Market	• **Digital Trade** • **Gigabit** broadband, Metaverse • **Ubiquitous** Connectivity, computing, quantum cloud • **Pervasive** Intelligence, Autonomous systems • Renewable energy, **Green** ICT • **Data security governance** for data monetization

Failure to cooperate and develop is the biggest security threat and risk!

Annex A

Normative references

Item	Terms /Standards	Title and Source
1	Digital First Economy	https://www2.abaconline.org/assets/2022/Publications/Digital%20First%20Economy.pdf
2	Global Industry Vision Exploring the Intelligent World 2030	https://www-file.huawei.com/-/media/CORP2020/pdf/giv/Intelligent_World_2030_en.pdf
3	Cybersecurity Workforce Study 2023	https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4
4	The ASEAN Digital Innovation Programme (ADIP):	https://www.aseanfoundation.org/asean_digital_innovation_programme
5	ASEAN Digital Literacy Prohramme	https://www.digitalclassasean.org/
6	ASEAN Seeds for the Future:	https://www.aseanfoundation.org/asean_seeds_for_the_future
7	GSMA Mobile CKB	https://www.gsma.com/security/5g-cybersecurity-knowledge-base/
8	OIC-CERT 5G Cyber Security Framework	https://www.oic-cert.org/en/events/5g/index.html#.YodGRKhByUk
9	United Nations General Assembly A_77_92	https://digitallibrary.un.org
10	Policy paper The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023	https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023
11	The Bletchley Declaration: Shaping the Future of AI Together	https://opengovasia.com/the-bletchley-declaration-shaping-the-future-of-ai-together/
12	RIDE MADANI:	https://www.thestar.com.my/business/business-news/2023/11/21/mcdc-launches-ride-madani-initiative-attracts-rm100bil-in-investments
13	Indonesia Cloud Service Security and Data Security Governance	https://bssn.go.id/wakil-kepala-bssn-luncurkan-buku-tinjauan-strategis-keamanan-siber-indonesia-teknologi-cloud-dan-tata-kelola-data/
14	Uniting for an Inclusive Digital Future	https://www.apac-business.com/companies/corp-events/uniting-for-an-inclusive-digital-future-huawei-asean-foundation-and-seameo-empower-asia-pacifics-young-tech-talents/
15	ASEAN Cybersecurity Skilling Programme	https://www.aseanfoundation.org/asean_cybersecurity_skilling_programme
16	A multi-stakeholder High-Level Advisory Body for Artificial Intelligence will report on global AI governance by the end of 2023	https://unu.edu/article/secretary-general-antonio-guterres-convenes-critical-body-debate-global-governance
17	ISO/IEC FDIS 42001	ISO/IEC FDIS 42001 Information technology Artificial intelligence Management system (ISO/IEC JTC 1/SC 42): https://www.iso.org/standard/81230.html
18	ISO/IEC 38507:2022	ISO/IEC 38507:2022 governance implications of the use of AI, https://www.iso.org/standard/56641.html
19	Digital Trade Opportunities and Challenges,	https://www.wto.org/english/tratop_e/devel_e/digital_trade2022_e.pdf
20	ASEAN-China FTA	https://fta.miti.gov.my/index.php/pages/view/asean-china?mid=33
21	Digital Economy Partnership Agreement (DEPA)	https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement
22	ASEAN Digital Economy Framework Agreement	ASEAN Digital Economy Framework Agreement, https://asean.org/wp-content/uploads/2023/09/Framework-for-Negotiating-DEFA_ENDORSED_23rd-AECC-for-uploading.pdf
23	Initiative on International Trade and Economic Cooperation Framework for Digital Economy and Green Development	https://www.mfa.gov.cn/eng/zxxx_662805/202310/P020231020384764366957.pdf
24	Malaysia Data Security Governance Reference Book	https://pikom.org.my/2023/DSG/Malaysia_Data_Security_Governance_Reference_Book.pdf
25	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
26	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
27	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/
28	IEEE P3141	IEEE P3141 Standard for 3D Body Processing, https://standards.ieee.org/ieee/3141/10825/
29	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
30	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
31	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
32	ISO/IEC 21823-4:2021	ISO/IEC 21823-4:2022 Internet of things (IoT) — Interoperability for IoT systems — Part 4: Syntactic interoperability, https://www.iso.org/standard/84773.html

33	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
34	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
35	OWASP IoT verification standard	OWASP IoT verification standard, https://owasp.org/www-project-iot-security-verification-standard/
36	ISO/IEC JTC 1/SC 37	ISO/IEC JTC 1/SC 37 Biometrics, https://www.iso.org/committee/313770.html
37	ISO 62304	ISO 62304 Medical device software — Software life cycle processes, https://www.iso.org/standard/38421.html
38	ISO 14971	ISO 14971 Medical devices — Application of risk management to medical devices, https://www.iso.org/standard/72704.html
39	ISO/IEC TR 24028:2020	ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence, https://www.iso.org/standard/77608.html
40	ISO/IEC 20546:2019	ISO/IEC 20546:2019 Information Technology-Big Data-Overview and vocabulary, https://www.iso.org/standard/77608.html
41	ISO/IEC TR 20547:2020	ISO/IEC TR 20547:2020 Information Technology-Big data reference architecture, https://www.iso.org/standard/71275.html
42	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
43	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
44	TC590	TC590 National Technical Committee for Standardization of Blockchain and Distributed Accounting Technology, https://std.samr.gov.cn/search/orgDetailView?tcCode=TC590
45	ISO/IEC TR 23188:2020	ISO/IEC TR 23188:2020 Information Technology-Cloud computing-Edge computing landscape, https://www.iso.org/standard/74846.html
46	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
47	3GPP Release15/16/17/18	3GPP Release15/16/17/18, https://www.3gpp.org/specifications-technologies/releases
48	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
49	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
50	NESAS|SCAS	NESAS|SCAS, https://www.gsma.com/security/network-equipment-security-assurance-scheme/
51	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
52	ISO/IEC 19790:2012	ISO/IEC 19790:2012 Information Technology-Security techniques-Security requirements for cryptographic modules, https://www.iso.org/standard/52906.html
53	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
54	Cloud Controls Matrix (CCM)	Cloud Controls Matrix (CCM), https://cloudsecurityalliance.org/research/cloud-controls-matrix/
55	CIS	CIS Critical Security Controls Version 8, https://www.cisecurity.org/controls/v8
56	SOC 1/2/3	SOC 1/2/3, https://www.aicpa.org/cpe-learning/course/soc--for-cybersecurity-certificate-program
57	NIST CSF	NIST CSF, https://www.nist.gov/cyberframework
58	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
59	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
60	ISO/IEC 27002:2022	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, https://www.iso.org/standard/75652.html
61	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
62	ISO/IEC 27005:2018	ISO/IEC 27005:2018 Information technology-Security techniques -Information security risk management, https://www.iso.org/standard/75281.html
63	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
64	COBIT	COBIT,https://www.isaca.org/resources/cobit
65	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
66	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
67	ISO/IEC 38500:2015	ISO/IEC 38500:2015 Information technology — Governance of IT for the organization,https://www.iso.org/standard/62816.html
68	ISO/TC 309	ISO/TC 309 Governance of organizations, https://www.iso.org/committee/6266703.html
69	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
70	ISO/IEC 29100:2011	ISO/IEC 29100:2011 Information technology-Security techniques-Privacy framework, https://www.iso.org/standard/45123.html
71	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
72	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
73	ISO/IEC 29101:2018	ISO/IEC 29101:2018 Information technology-Security techniques-Privacy architecture framework, https://www.iso.org/standard/75293.html
74	CSA CoC for GDPR Compliance	CSA CoC for GDPR Compliance, https://cloudsecurityalliance.org/privacy/gdpr/code-of-conduct/
75	United Nations Commission on International Trade Law	https://uncitral.un.org/en
76	GAIA-X and IDS	GAIA-X and IDS, https://internationaldataspaces.org/publications/most-important-documents/

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
instagram.com/pikom_official
facebook.com/MYPIKOM
linkedin.com/in/pikom

www.pikom.org.my