Proposals for the Global Digital Compact

By Cloud Security Alliance Greater China Region

February 07th, 2023

CSA GCR cloud security alliance GREATER CHINA REGION ®

Overview

Digital development is a global trend. With the rapidly progress and spreading of the digital technology, more and more people's lives and work relies on digital technology. As an important part of digital development, digital security significantly ensures the security and stability of the digital environment. The Global Digital Contract is a framework, providing all international cooperations with a common principle for an open, free and secure digital future. Digital security is a significant part of the Global Digital Contract, with the purpose to ensure the security of the digital environment, the protection of privacy, and the sustainable development of digital technologies.

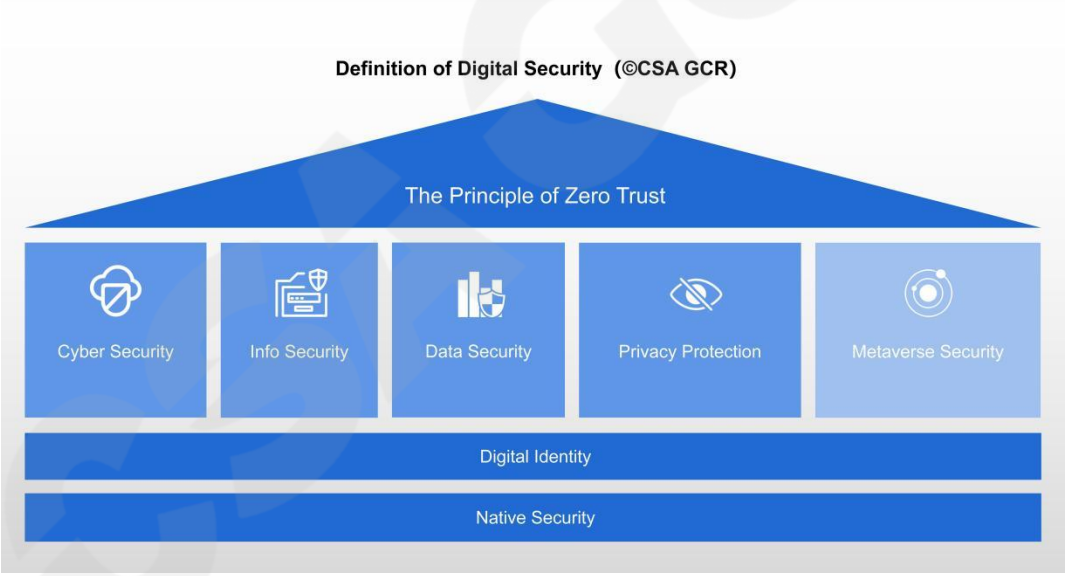
CSA GCR proposed a digital security framework and released a global digital security report, and the report provided recommendations in four directions: standards, cooperation, rights and interests, and applications. CSA GCR recommends to establish globally unified digital security standards, improving the system of compliance and regulatory rules for the whole process of globally recognized data, and strengthening cooperation among countries to jointly deal with human digital risks. Meanwhile, it is necessary to build a system to protect the rights and interests of data owners, enabling the using of data on globalling in the legal and compliant methods, and promoting the application of digital technology safely.

Table of Contents

Chapter 1 | Global Digital Security Framework – Top-level Architecture

1.1 | Definition of digital security

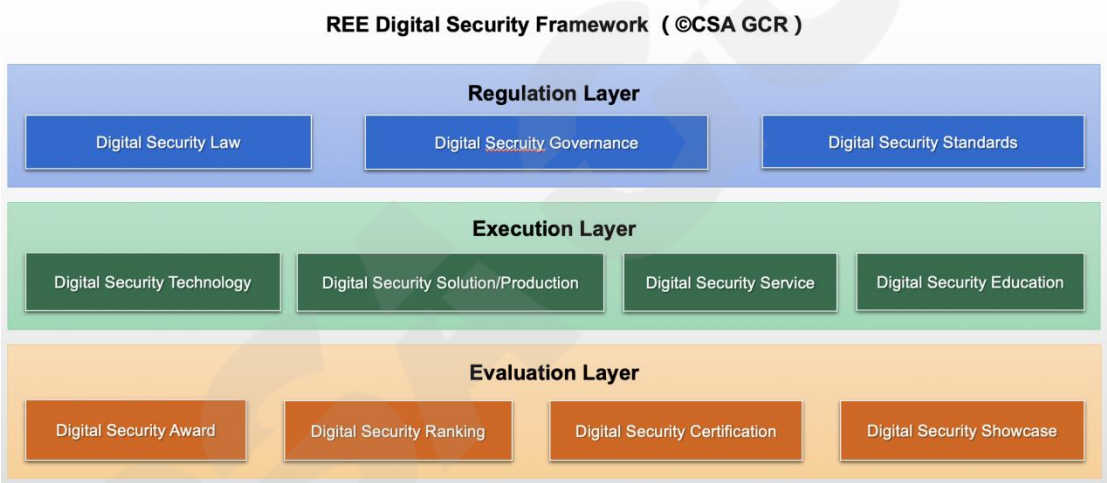
Digital security refers to the collection of all security elements, behaviors and states related to digitalization in the Digital Times, including not only the security of the digital economy, but also the use of digital technology in the field of security. Digital security takes digital identity as the core and native security as the base, covering information security, network security, data security, privacy protection and other fields or scenarios, and can be extended (such as Metaverse security). In addition, digital security also includes the use of digital technology to ensure the physical security of digital infrastructure. Although digital security pays more attention to digital economy and digital technology, it is also similar to Cybersecurity which emphasizes national cyber sovereignty in terms of law, standard and technology. The definition of digital security is shown in figure 1:



- **The Principle of Zero Trust**：zero trust is the highest digital security strategy, through the digital security technology stack used to protect the safety of data in the digital world.
- **Cyber Security**: to ensure the security of the hardware and software of the network system, responsible for CSO、CTO etc.
- **Information Security:** to ensure the security of all valuable information, responsible for CISO、CIO etc.
- **Data Security**: to ensure the security and compliance of data throughout the life cycle, responsible for CDO、CIO、CISO、CSO etc.

- **Privacy Protection**: protect users' privacy and personal information, responsible for CPO, DPO etc.
- **Metaverse Security**: to ensure the security of parallel universes which are born and blended by virtual and real carried in digital form, and it is also the main expansion field of digital security in the future.
- **Digital Identity**: as a base for connecting security and business, it provides digital identification, authentication and access lifecycle management for all people, digital people, objects, devices, etc.
- **Native Security**: native security includes the native security of systems involved in cloud computing, big data, AI, 5G/6G, IoT, blockchain, quantum computing and other emerging technologies. It is the base of digital security and needs the support of hardware trust roots.

1.2 | REE digital security framework



REE Digital Security Framework

- **Regulation Layer：** The rule layer is the strategic guidance of the digital security framework, which mainly includes digital security law, digital security governance, digital security standards and so on. This layer needs to solve the problems of digital security laws, regulations, rules, policies, supervision and standards, so as to provide strategic guidance for the digital security construction and compliance governance of the organization.
- **Execution Layer：** the enforcement layer covers all the resources / tools needed for the landing of the rule layer and the specific actions for the use of these resources / tools, including the implementation of digital security technology, digital security solutions / products, digital security services, digital security education and so on. This layer needs to solve the problems such as the research and progress of digital security technology, the development and application of

digital security solutions / products, the development of digital security services (such as security consulting, security operations, etc.), the cultivation of digital security talents, and so on. It is the core for an organization to achieve its digital security goals.

- **Evaluation Layer:** the evaluation layer evaluates, verifies and examines the digital security maturity of the organization, including digital security awards, digital security ranking, digital security certification, digital security cases and so on. This layer needs to continuously evaluate the digital security capability of the organization through security certification / audit / evaluation, so as to promote continuous improvement and improvement, and achieve a security closed loop from rules, implementation, evaluation to improvement. In addition, relevant market promotion and guidance is carried out through digital security awards, digital security rankings / quadrants and digital security excellent cases sharing, so as to promote the development of digital security industry.

Chapter 2 | Digital Security and Data Protection Domain – Core Principles and Key Actions

2.1 | One unified global digital security standard to maintain the consistency, complementarity, and interoperability of digital security

Recommendation for actions:

- Governments should adopt a comprehensive framework at the national level to manage various country-level digital security risks, and strengthen them together in a managed way. The framework and implementation policy should be transparent, and the digital security framework provided by the CSA GCR will be a reliable reference for developing the comprehensive framework. A well-established and transparent government digital security framework should be regularly reviewed by any authorized stakeholders from within and outside the country, and it can be improved based on experience and best practices, and it can be benchmarked and measured by one international standard where it's possible
- Based on that, the United Nations should provide a platform to show the status of different countres' digital security risk assessment, and ensure it will be well balanced among different competing policy objectives.
- International rules and digital technology standards in data flow, data security, certification, evaluation, and digital currency should be formulated or revised according to the Global Digital Compact

2.2 | Strengthen international cooperation to address common digital risks

Recommendations for Action:

- If countries need to perform data forensics services across borders for law enforcement, they should resolve it through international judicial assistance channels or other relevant multilateral and bilateral agreements.
- The conclusion of bilateral agreements on cross-border data collection between countries must not infringe upon the judicial sovereignty and data security of any third country.
- Take coordination and cooperation on managing challenges and threats to global information security and data security.
- Take measures to prevent and manage the use of information technology for cybercrime and terrorist activities at the national, regional and global levels

2.3 | Establish the basic data protection system to protect the rights and interests of data owners, and enable the legitimated use of data globally

Recommendations for Action:

- It is recommended that the United Nations takes the lead in establishing a secure and well-managed mechanism for cross-border data transfer. The UN should take a great effort to improve the globally consistent authorization mechanism for protecting rights to public data, enterprise data, and personal information data. The UN should notice the trend in which data as a new productive factor could be transferred and even trade globally in the future, but the international norm in this area is scarce. In the future, the UN should play a central role in carrying out international exchanges and cooperation in data interaction, business interoperability, mutual recognition of supervision, and service sharing, and promoting the construction of cross-border digital trade infrastructure.
- Countries should respect the sovereignty, jurisdiction and data security management of other countries, and shall not directly access data located in other countries from enterprises or individuals without the permission of the laws of other countries.
- It’s not allowed to misuse information technology to destroy critical infrastructure or steal important data from other countries, as well as the use of information technology to engage in acts that endanger the national security and public interests of other countries.

- All countries undertake to take measures to prevent and stop the use of the Internet to infringe on personal information, and oppose the misuse of information technology to engage in large-scale surveillance against other countries and the illegal collection of personal information of citizens of other countries.

2.4 | Establish a secure, controllable, and resilient data governance system to promote the application of digital technologies securely

Recommendations for Action:

- Improve the compliance and regulatory system in which the whole data lifecycle process is globally recognized.
- Information technology products and service suppliers shall not have backdoors in products and services to illegally obtain user data, control or manipulate user systems and equipment.
- Information technology enterprises should not take advantage of users' loyalty to products to seek improper benefits, and force users to upgrade systems or replace them. The product supplier undertakes to inform partners and users of the security defects or vulnerabilities of the product in a timely manner and propose remedial measures.
- Supply chain security is the foundation for the stable operation of global digital networks and key facilities, and is of decisive significance for promoting network interconnection and benefit. Network security vulnerabilities are an important risk to supply chain security, and the vulnerability management of general and basic network applications should be considered as a global public product, and the network risk of security vulnerabilities should be reduced through a coordinated manner, overall rather than partial, universal rather than different.

Chapter 3 | Introduction to Cloud Security Alliance Greater China Region

Cloud Security Alliance (CSA), an international technical standards organization in the field of network security, was formally established in 2009, and is committed to defining and improving the industry's understanding of the best practices of cloud computing and next-generation digital technology security, and promoting the development of digital technology and security industry.

The International Cloud Security Alliance Greater China Region (CSA GCR), as one of the four global regions of CSA (the other regions are the Americas, Asia-Pacific and Europe-Africa regions), was officially registered in Hong Kong in 2016, and registered and landed in 2021 with the support of the Ministry of Industry and

Information Technology of China, the Ministry of Public Security and the Office of Internet Information Technology. It is the first and only international NGO registered and registered in China in the field of network security.

The CSA Institute is the core competitiveness of CSA to maintain its leading and authoritative position, and its research agility, professionalism and integrity have been recognized by the industry. The Institute has 83 research working groups to carry out comprehensive research on cloud computing and next-generation digital technology security. The Institute outputs more than 500 research results, more than 60000 registered experts and 130000 community professionals.

There are 12 research working groups of CSA GCR, which have output more than 100 industry guides in the direction of cloud security, Internet of Things security, data security, zero trust, privacy technology, and more than 1000 registered experts in China, including academicians, professors, public institution experts, scientific researchers, enterprise technology executives, security experts and other experts who have worked for more than 10 years.

The CSA SECtember is the largest international conference on cloud security. CSA GCR Congress, EMEA Congress and APAC Congress are important conferences in all regions.

3.1 | CSA release standards

No.	Standard Name	Standard Type
1	Cloud Controls Matrix (CCM)	International Standard
2	Cloud Computing Security Technology Requirements (CSTR)	Industry standard
3	Cloud Security Capability Maturity Model Integration Assessment Guidance（CS-CMMI）	Industry standard
4	Software-Defined Perimeter (SDP) Specification	International Standard
5	Cloud Application Security Technology (CAST)Specification	Industry standard
6	Cloud Native Security Technology (CNST)Specification	Industry standard
7	Internet of Things (IOT) Security Specification	Industry standard
8	Basic Information Security Test Benchmark of	Industry standard

	Mobile App	
9	Smart Contract Security Technical Specification	Industry standard
10	Zero Trust Maturity Model	Industry standard

3.2 | CSA release courses

- Certificate of Cloud Security Knowledge (CCSK)
- Advanced Cloud Security Expert (ACSE)
- Certified Cloud Penetration Test Professional (CCPTP)
- Advanced Cloud Security Practitioner (ACSP)
- Certificate of Cloud Auditing Knowledge (CCAK)
- Certified Cloud Security Management Professional (CCSMP)
- Certified Zero Trust Professional (CZTP)
- Certified Blockchain Professional(CBP)
- Certified Data Security Professional(CDSP)
- Certified Data Protection Officer(CDPO)
- GDPR Lead Auditor

Acknowledgement

Amandeep Singh Gill, The Under-Secretary-General of The United Nations and Special Envoy for Science and Technology of the Secretary-General, supported and guided the CSA GCR to participate in this work. Peter Major, Chairman of the Commission on Science and Technology for Development and Honorary President of the United Nations Digital Security Alliance, supported and guided the CSA GCR to carry out digital security work. Chen Zhimin, Deputy Director of the CPPCC Social and Legal Committee and Chairman of the China Association for Friedship, supported and guided the CSA GCR to carry out data security research. Cyberspace Administration of China , the Ministry of Industry and Information Technology, The Ministry of Public Security of the People's Republic of China and the leaders of relevant departments supported and guided the development of the CSA GCR, and the member units and experts of the Alliance actively participated in and strongly supported the research work of the CSA GCR.

Members of the editorial board of the Proposal for the Global Digital Compact:

Li Yuhang, Lv Lixiao, Jia Liangyu, Guo Pengcheng, Xu Mudi, Chen Benfeng, Zhang Miao, Yuan Hao, Gu Wei, Ou Jianjun, Shi Yuhang, Wang Yumeng, Ye Xiaoqian, Zhang Wenjuan