Enterprise data security compliance strategy: A study based on typical cases

Yinghui Xu[1, *], Xi Chen[1], Chuang Li[1], Lianzhu Ge[1], Haiyan Zhao[1], and Tianying Jiang[2]

[1]China Electric Power Research Institute Co., Ltd, Beijing, 100192, China
[2]Beijing Wuzi University, Beijing, 101149, China

Abstract. Data security compliance management is the fundamental premise that data application does not infringe on the interests of countries, enterprises and individuals. It is an important foundation for realizing the driving role of data elements. Based on the data security compliance management practices of typical enterprises at home and abroad, this paper summarizes the excellent practices of leading demonstration enterprises, and proposes six key strategies for enterprise data security compliance, including classification of typical data application scenarios, analysis of key links of data security compliance application, formulation of data security compliance application management system and standards, optimization of data security compliance application process mechanism, formulation of whole-process management measures of data security compliance, and improvement of data security compliance guarantee mechanism, as to provide references for the research and construction of enterprise data security compliance management system.

1 Introduction

Data security compliance management is a necessary requirement for implementing national data security strategy. Cyber attacks targeting data are becoming more and more frequent worldwide, challenging the security of sovereign states. Ensuring data security and clarifying data sovereignty has become an urgent strategic deployment for all governments around the world today [1]. Enterprise data involves state secrets, trade secrets and personal information, which is extremely sensitive. So we must strictly abide by the legal provisions of the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, etc., establish a strong and efficient data security compliance management system, comprehensively identify data security compliance risks, and improve and perfect the control mechanism, to ensure network and information security.

Data security compliance management is an inevitable choice to adapt to the regulatory requirements of the new situation. In the face of increasingly stringent regulatory requirements, enterprises must take the lead in the protection of state secrets, business secrets, personal information and other relevent fields, strengthen the data security compliance management capacity and build the whole chain of data security compliance management system.

Data security compliance management is a strong guarantee to promote the digital transformation of enterprises. With the rapid development of digital economy, coordinating data security and development has become the core and focus of sustainable and healthy development of digital economy [2]. It is shown that the digital transformation of enterprises has been accelerating, data opening has been deepening, various data application innovations emerge in an endless stream. Therefore, effective data protection and efficient data application have simultaneously become important aspects of enterprise data asset operation [3]. In the process of digital transformation of enterprises, it is urgent to effectively solve the contradiction between data security compliance and data innovation applications, so as to avoid slowing down the pace of data application due to the fear of violations.

2 Typical practices of enterprise data security compliance management

Focusing on the leading demonstration of enterprises, this paper selects China Petrochemical Corporation (SINOPEC), Industrial and Commercial Bank of China (ICBC), China Mobile Communications Corporation (CMCC), Huawei Cloud, Ant Financial Services Group (AFSG), Google, General Electric (GE), etc., to conduct in-depth analysis and comparative analysis. The main practices and inspirations are illustrated as follows.

* Corresponding author: xcfw@epri.sgcc.com.cn

2.1 Carry out the top-level design of data security compliance management and form the organizational guarantee of data security compliance management

The first is to build a data security compliance management system. SINOPEC comprehensively carried out data security management, completed the overall design of data security management system and issued SINOPEC Data Operation and Management Measures. CMCC has established and improved its data security system, which involves six aspects of data security strategy management, operation, technology, evaluation and service, and has realized Closed-loop management through establishing organization, rules and regulations, construction means, supervision and inspection. China Unicom (CHU)' s big data took "data security" as the core and built an independent and controllable big data life cycle security system from four aspects: big data security technology system, security strategy system, security organization system and security operation system. On the basis of complying with regulations and regulatory requirements, drawing lessons from international and industrial data security standards and referring to industrial excellent practices, Huawei Cloud has established and operated a set of perfect, highly credible and sustainable data security governance system from five aspects of organizational responsibilities, policy requirements, process guidance, technical tools and measurement verification, effectively protecting data of customers.

The second is to establish an organizational structure for data security compliance. SINOPEC set up a data governance committee of the group company, and defined its management responsibilities in data structure validation, data use principles and data security responsibility system. Huawei Cloud has set up a top-down data security management responsibility system, which is the foundation for protecting the company's and customers' data on the cloud. The system includes decision-making layer, management layer, executive layer, supervision layer and support layer, promoting the effective implementation of data security work layer by layer. Xiaomi Corporation has established a data compliance organizational structure, including three levels: the information Security and Privacy Committee, the Committee Office, the Business Unit Security and Privacy Committee. In some groups of GE, there are legal departments and compliance departments. The legal departments focus on the management and implementation of contracts and other legal acts, while the compliance department focus on the compliance with laws and regulations, and the implementation and optimization of the company's rules and regulations. The compliance department is composed of compliance personnel with different backgrounds such as law, audit technology, etc., which is more conducive to connection between business practices and compliance requirements.

The third is to cultivate a cultural atmosphere of data security compliance. Google emphasizes the cultivation of the overall data security culture of employees and enterprises, instills the awareness of data security in employees from the whole process of enterprise operation activities; Investigates the security background of employees in combination with job requirements, conducts continuous security training for employees; Regularly arranges internal meetings and activities related to information security and privacy and conducts targeted training according to specific positions and functions. Huawei requires employees, partners and external consultants to strictly follow the requirements of data security policies and receive security training so that the relevant requirements of security policies can be integrated into the whole organization.

2.2 Improve the guidance of data security compliance management system and promote the release of data security compliance management standards

On the one hand, improve the construction of data security compliance system. SINOPEC issued SINOPEC Network Security Management Measures, defining the management requirements for data security and personal information protection. In order to ensure privacy security, AFSG has formulated more than 30 systems and regulations such as the Privacy Protection System, the General Principles of Data Security Management and the Data Classification Specification, making them an integral part of business activities.

On the other hand, promote the standardization of data security compliance. CMCC is committed to promoting the practical experience of standard sharing, promoting the consensus of the whole industry and society. Its "vault mode" technology, Guidelines for the Implementation of Big Data Security Protection in Telecommunications, Guidelines for the Implementation of Big Data Security and Privacy and other more than ten achievements have been established or published in ISO/IEC, ITU-T, TC260, CCSA and other important standard organizations at home and abroad. ICBC participated in the construction of a number of data security-related standards in the industry and played the leading role in compiling guiding documents such as the Technical Specification for Federal Learning Finance Application, the White Paper on Financial Data Protection and Governance, the White Paper on Federal Learning Technology, the Finance Application Current Situation and Implementation Guidelines of Multi-party Secure Computing, etc. Tencent has been actively participating in the customization of industry norms, promoting the standardization of data security and personal information protection in combination with practical experience. It has participated in customizing of guiding documents such as Personal Information Security Norms, Personal Information Impact Assessing Guidelines, Personal Information Security Engineering Guidelines, Basic Standards for Collecting Personal Information by Mobile Internet Applications (APP), Security Capability Requirements for Big Data Services, Big Data Security Management Guidelines and Implementation Guidelines for Big Data Security Protection in Telecommunications.

2.3 Clarify the enterprise data classified and graded management and control standards, enhance the technical ability of sensitive data security protection

First of all, implement data classification and hierarchical control. Since 2016, CMCC has started the practice of data classified and graded management in an all-round way, compiled the implementation guide of classification and grading, dividing the data into four categories, four levels and four forms (original data, desensitized data, labeled data and group data) for differentiated management and control, which was popularized and applied in the whole group. SINOPEC divided the management data into four levels: core important level, important level, internal open level and external open level, and controlled the development authority and data entitlement, realizing the classified and graded management and protection of data.

Secondly, strengthen the identification and protection of sensitive data. According to the data classification and grading strategy, ICBC automatically identified sensitive data and results of classification, assisting data security marking. The identification results are used for power control, desensitization, auditing and other scenarios. Using natural language processing, combined with regular matching, keyword matching, text classification, similarity AI model, it built intelligent data recognition capability. Through the on-premises desensitization algorithm and user-defined policy configuration, ICBC can provide unified desensitization services, greatly improving the deployment efficiency of data desensitization strategies and the availability of desensitization data. In accordance with the principles of minimizing collection and permission, SINOPEC protects personal information, realizing sensitive information monitoring and protection of important information systems through content monitoring and desensitization. Researches on risk assessment methods and tool testing for data security and personal information protection are carried out, for important information systems, to lay the foundation for data security risk assessment. In the case of sensitive data processing on the customer cloud, Huawei Cloud is able to encrypt and compute sensitive data based on homomorphic encryption technology. In this way, the original content of the data can not be accessed by anyone while the data is being processed.

Thirdly, strengthen the preventing construction of data leakage. Aimed at big data platform, mail system, Internet access, internal document flow and other application scenarios, SINOPEC has deployed network DLP, document security, online behavior management and other technical protection measures. It has the capabilities of keyword and behavior baseline interception, screen shot watermark deterrence, access to audit and other capabilities to effectively control internal data leakage; It can conduct strong authentication and permission control for privileged accounts of system, security operation and maintenance and key data operations; The multi-factor and certificate authentication, encryption and decryption, desensitization, digital signature and other capabilities of information systems are brought into the control scope of the unified identity and password service platform, so as to achieve the compulsory management of basic data security capabilities and data security operation. GE has established a unified identity and access management (IAM) system to develop standardized process specifications for the access of large amounts of data and the transfer of different data within its business scope, which reduced the number of audit accessing team members, enabling the enterprise to ensure that the access of personnel in various fields and functions meets internal requirements. At the same time, different security lines are set up according to the needs of data security in various fields.

2.4 Strengthen data security compliance protection assessment and inspection, develop data security compliance monitoring and early warning mechanism

The first is to strengthen data security compliance assessment and inspection. CMCC regularly carries out data security assessment and inspection on all units of the group, establishes working standards for data security compliance assessment, which sets the threshold for problem inventory and responsibility investigation. In order to ensure the effectiveness of data security requirements, Huawei Cloud evaluates the effect of data security governance through two major measures: First, it establishes a complete measurement system to continuously evaluate and measure the effect of data security governance. Second, it promotes construction, through the three lines of defense of data security supervision, to ensure the real and credible implementing effect of security requirements. Zhongxing Telecom Equipment (ZTE) uses the data protection impact assessment system to assess the types of personal data collected during the research stage and analyze the privacy protection measures in terms of permissions, logs, encryption and anonymity; It evaluates, processes and transmits personal data that meet the compliance requirements, guides products and services to take compliance measures, ensuring personal data processing activities, that have a significant impact on personal rights and interests, meet the compliance requirements.

The second is to promote monitoring and early warning of data security compliance to be normalized. CHU has built a big data security monitoring and auditing system for violations and exceptions in the data life cycle. With user operation behavior as the core, CHU has achieved big data platform data asset operation security monitoring and auditing through the whole network tracking and correlation analysis. Google uses Cloud Health to carry out unified management of data from all sources of the platform, then utilizes cloud health driven automatic functions to monitor and alert users who exceed their permissions and whose data access audit logs are accessed by unknown parties, so as to realize 24-hour monitoring of the cloud environment and remind users of violations or possible violations of

data governance policies at all times. CMCC initiated the "Moms' Class" and the national centralized management mode of malicious information, built a systematic data security management system, independently developed a big data anti-fraud monitoring platform, and continued to strengthen the interception and management of illegal information through public opinion monitoring, data mining, trend analysis and other technical means. New loopholes, taken advantages of by the Criminals to escape from blocking, such as regional differences, system differences and time differences, have been effectively solved.

2.5 Improve the control mechanism covering the full life cycle, ensure the safety and compliance of data operation of all links

First is data collection. ICBC identifies and authenticates data sources through digital signature and other technologies, and classifies and grades the collected data. AFSG system can monitor the whole process of data collection, and if any risk is found without user's authorization, it will start an early warning or terminate it directly. CMCC's Wutong big data platform collects data through sensitive data identification, review and control and encrypted network channels to ensure data security in the collection process.

Second is data transmission. ICBC realizes the secure transmission of data through the trusted physical channel, encrypted transmission and communication protocol. CMCC's Wutong big data platform adopts control measures such as strict review of network policy, encrypted transmission of files and data, internal encrypted network channels, and transmission log retention and audit to ensure the safe transmission of data.

Third is data storage. ICBC guarantees the integrity of data storage through encryption and other technologies, and formulates data backup and recovery strategies according to the security level of data and system. CMCC's Wutong big data platform adopts control measures such as signing confidentiality agreement, 4A access to the production system, encryption and storage of sensitive data, and data backup and recovery mechanism to ensure data storage security. Huawei Cloud uses AES to encrypt static data stored in the cloud infrastructure, effectively protecting data security on the cloud platform.

Fourth is data use. ICBC has widely applied data control, data desensitization and other technologies to ensure data security, and explored the use of multi-party secure computing and federated learning technology to exert the efficiency of data fusion and linkage under the condition that the data is not out of the domain, so as to realize the data available and invisible. AFSG uses technology to carry out intelligent classification of data, conducts special identification and desensitization of sensitive data to prevent information leakage in the use stage of data, and establishes fine-grained permission control in accordance with the "minimum sufficient" principle.

Fifth is data sharing. In the data sharing stage, AFSG conducts real-time monitoring of abnormal data calling behavior, and restricts partners to obtain user's consent before accessing user's data. CMCC's Wutong big data platform adopts control measures such as security review of sensitive data and strict control of non-opening of level 4 sensitive data to ensure the security of data sharing.

Sixth is data destruction. At the end of the data life cycle, ICBC forms a closed loop through data cleaning and destruction of storage media. Huawei Cloud implements data security destruction at the level of platform and physical media destruction. At the platform level, Huawei Cloud deletes specified data and all copies thereof. In terms of physical media destruction level, in order to ensure data security at the end of the data center media life cycle, Huawei Cloud implements a comprehensive storage media disposal mechanism based on relevant industry standards.

3 Key strategies for enterprise data security compliance

First, classify typical data application scenarios. It is of great necessity to ensure the compliance of the whole process of enterprise data based on scenario driving [4]. The nature, type and application mode of data are determined through specific scenarios; the data rights and interests of relevant subjects are defined according to the reasonable expectations of all parties in specific scenarios. The scenarios are classified according to the similarity of data security compliance requirements in specific scenarios, and then analyze the basic paradigms of data security compliance application in each type of scenario.

The second is to analyze key links in the application of data security compliance. The whole process of data processing generally includes data collection, storage, use, processing, transmission, provision, disclosure, deletion, etc. According to the information data processing rules stipulated in the Personal Information Protection Law and the Data Security Law, the key links of data security compliance application can be summarized in typical scenarios as total four links of collection link, storage link, use link, processing link and external supply link.

The third is to develop data security compliance application management system and standards. Enterprise data compliance application should establish basic principles of data processing activities such as legal compliance, consent notification, legitimate purpose and minimum necessity [5]. Data security management should pay attention to the processes of access, review, verification, authorization and monitoring, formulate general systems of classification, data security, data risk assessment and key protection of important data, and formulate differentiated strategies in each link. Key points include data compliance management rules, data compliance risk assessment criteria, data classification and grading standards, data security emergency response plans, etc.

The fourth is to optimize data security compliance application process mechanism. In the collection link, one enterprise should update the privacy policy in time, fully fulfil the obligation of notification and the collection content should be minimum necessary. In the storage link, one enterprise should establish the data quality management system, improve the security storage capacity, classify the data, reasonably set up the data storage period and handle the situation of deleting user's information, and the data leakage notification system should be established. In the link of use and processing, one enterprise should abide by the agreed content with users, and obtain the users' consent again when sharing data. When providing public services, an agreement should be signed with the user community or the government. In addition, reasonable approval procedures should be set up and fulfilled, and the legitimacy of entrustment should be ensured when accepting entrustment. In the external provision link, one enterprise should carry out data risk assessment, establish a negative list of data sharing, reduce data privacy risks by utilizing privacy enhancement technologies, enhance data confidentiality protection [6], and formulate differentiated strategies for providing data to the outside.

The fifth is to formulate the whole process of data security compliance management measures. In the prior stage, one enterprise should construct the enterprise data security compliance risk database, to determine the data risk level, carrying out the data risk identification. Based on the data security compliance risk database, conduct a comprehensive investigation of data security compliance risks and propose suggestions for improvement. In the middle stage, conduct data security compliance review, strengthen security control of key links such as information system construction, data acquisition, data operation and maintenance, internal sharing and opening to the outside world, summarize key points of review and update and improve them. In the post-event stage, establish the data security compliance emergency plan and violation incident reporting system, clarify the incident reporting and disposal process and time limit requirements, and take timely countermeasures to minimize risks and reduce losses. In the whole process, data security tools should be applied and upgraded, including security software, identity management technology, intrusion detection and defense software, physical isolation, and data encryption and desensitization, etc.

The sixth is to improve the data security compliance mechanism. Build a guarantee mechanism from the three aspects of team building, evaluating rewards and punishments, and tool empowerment, to firmly support the construction of data security compliance management system and ensure the realization of management objectives. In terms of team building, one is to perfect the staffing of data security and compliance management personnel, and carry out cultural construction such as case summary and course training. As for the evaluation of rewards and punishments, data security compliance management evaluation should be carried out, which is to reward excellent groups or individuals and deal with violations. In the aspect of tool empowerment, promote digital construction of safety compliance management, and solidify management requirements using technical measures, so as to standardize management processes and improve management efficiency.

4 Conclusion

With the improvement of data security compliance legislation and the normalization of data administrative law enforcement inspections, data protection actions are becoming more frequent. It is urgent for enterprises to strengthen construction in such aspects as classification of typical data application scenarios, analysis of key links of data security compliance application, formulation of data security compliance application management system and standards, optimization of data security compliance application process mechanism, formulation of whole-process data security compliance management measures, and improvement of data security compliance guarantee mechanism, as to ensure the safety and compliance of enterprise data operation.

Acknowledgments

This paper is a phased achievement of technical consulting project of China Electric Power Research Institute (Research on Data Security Compliance System of China Electric Power Research Institute, SGDK0000XZWT2207422).

References

1. J.Zhang. Systematic literature review of data sovereignty research in China[J]. Journal of Intelligence, 2022,41 (04): 128-134.
2. B.Chen, Z.Hu. The route of rule of law of coordinating data security and development under the digital economy[J]. Changbai Journal, 2021 (05): 84-93,2.
3. Y.J.Chi, F.Liu, J.Y.Qi. Construction of enterprise data protection maturity model under the background of digital transformation [J]. Journal of Intelligence, 2021,40 (09): 133-140.
4. H.He. Key issues and solutions of enterprise data security compliance governance[J]. Guizhou Social Sciences, 2022 (10): 126-133.
5. Y.Sun. Enterprise Data Compliance and Its Construction in the Digital Economy Era[J]. Hubei Social Sciences, 2022 (08): 119-128.
6. X.P.Sheng, D.S.Guo. Research on data security governance in open sharing of scientific data[J]. Library and Information Service, 2020, 64 (22): 25-36.