Research on Geological Data Security Governance System

Xiaohong Wu *[1, 2, a], Yi Yue [1, 2, b], Renbing Gao [3, c]

[1] Command Center for Integrated Natural Resources Survey, China Geological Survey, Beijing, China
[2] Development Research Center, China Geological Survey, Beijing, China
[3] Yantai Coastal Zone Geological Survey Center, China Geological Survey, Shandong, China

[a]e-mail: wxiaohong@mail.cgs.gov.cn
[b]e-mail: yueyi@mail.cgs.gov.cn
[c]e-mail: gaorenbing@mail.cgs.gov.cn

Abstract. Data is an important asset of an enterprise and a national basic strategic resource. Data security issues are increasingly prominent in the era of big data. Strengthening data security governance is not only an objective requirement of national supervision, but also a subjective requirement for the development of the data industry itself. Based on the practice of geological data security governance, proposes a geological data security governance framework consisting of a security management system, a technical system and an operation & maintanance system, and expounds the five steps of geological data security governance: asset sorting and evaluation, system construction, data classification, technical control and strategy optimization. Looks forward to the technological evolution of data security governance: scenario-based security protection, password-based data protection, and the use of artificial intelligence and other new technologies to optimize security solutions.

Keywords: data security; data governance; big data; geological cloud;

1 Introduction

Data is an important factor of production in the new era, and it is a national basic strategic resource [1]. Data is called the fifth largest factor of production after land, labor, capital, and technology [2].

Data has become the core asset of an enterprise. The development of big data has brought opportunities to enterprises, as well as data security challenges. While managing and using data, enterprises are bound to face significant security threats and management responsibilities. The issue of data security has always existed, but it has become more important and noticeable in the era of big data and artificial intelligence [3].

In recent years, China has successively released national data strategies such as the Action Outline for Promoting Big Data Development, the 14th Five-Year Plan for National Informatization Development, and the 14th Five-Year Plan for Digital Economy

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 67–74, 2022.
https://doi.org/10.2991/978-94-6463-108-1_9

Development, emphasizing the construction of a Digital China. With the development of the marketization of data elements, the huge value and significance of data have become prominent, but the development and utilization of data is a double-edged sword. When data creates value, it also faces risks such as data leakage, abuse, and tampering. In order to ensure data security, standardize data processing activities, and promote data development and utilization, the Data Security Law and the Personal Information Protection Law were officially promulgated, emphasizing both data development and security protection, and promoting the legal and rational use of data under the premise of ensuring security and privacy [4].

With the advent of the era of big data, the security architecture has gradually transitioned from the previous "network-centric" to "data-centric". Strengthening the research on network security issues in the big data environment and the network security technology research based on big data, and establishing and improving the big data security guarantee system have become an important task of enterprise security construction [5].

2 Data security governance requirements

The goal of data security governance is to ensure data confidentiality, integrity and availability (CIA). Confidentiality refers to ensuring that data is not accessed by unauthorized users, integrity refers to ensuring that data will not be tampered with without authorization, and availability refers to protecting the right of authorized users to legally access data [6]. Data security in a broad sense refers to a " data-centric " security system, emphasizing data protection in the entire data life cycle, and emphasizing data subject rights and privacy protection.

Data security risks mainly come from external organizations with targeted attacks, third-party partners, malicious insiders, and wrong operations by insiders. Data has high utilization value in the eyes of criminals. Targeted " hacker " organizations steal, tamper or attack data; unreliable partners may leak data resources, which making enterprises face huge data security risks; malicious internal users may steal data or destroy data systems for potential benefits, retaliation or competitive business; some internal personnel due to the low level of security skills, weak security awareness, negligence or accidental operation will also cause huge data risk.

When data security is damaged, it may lead to data leakage and abuse, or lead to the destruction of data reliability and accuracy, or cause data to be unavailable or inaccessible, which will cause serious threat and damage to the interests of individuals, organizations, society and even the country.

Strengthening data security protection is not only an objective requirement of national supervision, but also a subjective need for the development of the data industry itself. In recent years, with the promulgation of higher-level laws such as the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, the management and utilization of data elements are faced with rigid data security compliance requirements. The collaborative development of data utilization and data security will be a major problem in the development of China's data industry in a long time.

China Geological Survey (CGS) has established a number of professional data subcenters, built 98 core databases, and formed a large number of original data and result data of geological surveys. The geological data service platform represented by Geological Cloud has released more than 3,000 services to serve the public and professional users. While providing external services for geological data, ensuring the safety of geological data has become an important task in the construction of geological informatization.

The data life cycle is divided into six stages: collection, transmission, storage, processing, exchange and destruction [8]. In the life cycle management activities, CGS is faced with the dual requirements of data security risk protection and compliance supervision. In order to promote the balance between data use and data security, CGS has carried out data security governance from the organizational, institutional, technical and operational levels in accordance with relevant laws and regulations.

3 Geological data security governance structure

Data security governance is the various strategies, technologies and activities adopted to ensure data security, including the process of improving data security risk response capabilities from aspects such as corporate strategy, organizational construction, business processes, rules and regulations, technical tools, management, operation and maintenance. In order to control the degree of security risk or minimize the risk impact [6]. The governance process is a complete system that runs through the entire organizational structure from the top to the bottom, from the decision-making level to the technical level, from the management system to the tool support.

3.1 Geological data security governance system

Data security governance mainly focuses on the vulnerability of data security, and formulates targeted strategies for various security risks faced to reduce security risks or reduce losses caused by security issues. In the whole process of data security governance, the most important thing is to formulate an appropriate data security strategy [6].

The geological data security governance system is shown below. It aims at the safe use of geological data, based on security risks and strategies, guided by the management system, supported by the technical system, and managed by the operation and maintenance system. It is integrated into the management, technology and operation and maintenance process, and runs through the whole life cycle of geological data. Through the organic combination and interaction of systems, technologies, processes and personnel, the goal of data security governance is finally achieved.

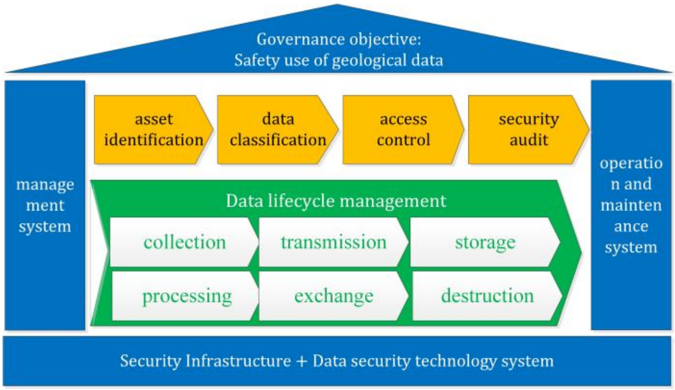

Fig. 1. Geological Data Security Governance System

The goal of security governance is to ensure the security of geological data, ensure the compliant use of data, and maximize data value through data flow. The security management system mainly includes organizational structure and personnel allocation, data security responsibility mechanism, security management system etc. The Security technology system mainly includes data asset identification, data classification and grading, data access control, security audit, etc. The security operation and maintenance system mainly includes dynamic protection strategy, data backup strategy, security education and training, etc. Security infrastructure focuses on data-related physical security and application security, including network layer security, cloud environment security, host layer security, application layer security, middleware security and data layer security. In the data security governance system architecture, the data security strategy is the core. It is formulated through the management system, implemented through the technical system, and released through the operation system to continuously ensure the safe development of data processing activities.

Data security includes the planning, establishment, and enforcement of security policies and processes to provide proper authentication, authorization, access, and auditing of data and information assets [7]. The security technology system is the key to the security governance system of geological data. All technology implementations revolve around "data-centered", which is the specific implementation of security policies in the system. The functions to be realized in the technical system are shown in the following figure.

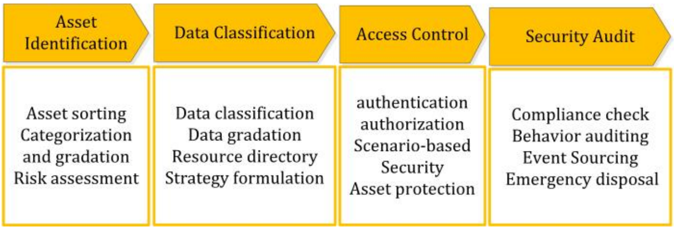

Fig. 2. Geological Data Security Technology System

The technology system provides the ability to make geological data visible, controllable, and manageable. Data managers have a comprehensive understanding of the status of data assets through information technology, find out the compositions of data, establish classification standards, and identify sensitive data. The security technology system provides the technical control means of each risk point in the whole life cycle of data, so that the data risk can be controlled, and ensure the confidentiality, integrity and availability of data. Through data operation and management, the dynamic security of data in different data environments is realized, and the data is well managed [6].

3.2 Security Governance Process

Geological data security governance works according to five steps of asset sorting and evaluation, system construction, data classification, technical control and strategy optimization, forming a closed-loop iterative data security governance framework and realizing spiral security capability improvement. The schematic diagram of data security governance is as follows.

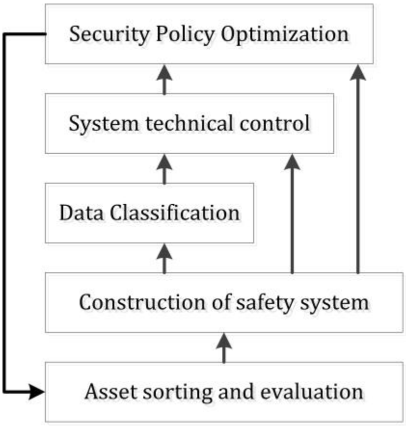
Security Policy Optimization
System technical control
Data Classification
Construction of safety system
Asset sorting and evaluation

Fig. 3. Five Steps of Data Security Governance Process

CGS sorts out the status quo of geological data assets and assess security risks. The data application, existing data management system, and data security status were investigated and sorted out. According to the classification of geological survey majors and disciplines, combined with the actual work, the resource catalog system and data classification standards have been established.

Based on the data application and data security management system of the previous step, combined with the data security laws and regulations promulgated by the state and higher-level units, and in accordance with the geological survey data security governance goals, CGS formulated data security management systems, management specifications, and process documents applicable to the geological survey industry, formed a security governance institutional architecture, as shown below. Combining the safety system with the resource catalogue and classification and grading norms, the developed process and system norms are transformed into practical safety management strategies, which are applied to the management process of the geological cloud platform and implemented in all aspects of data management.

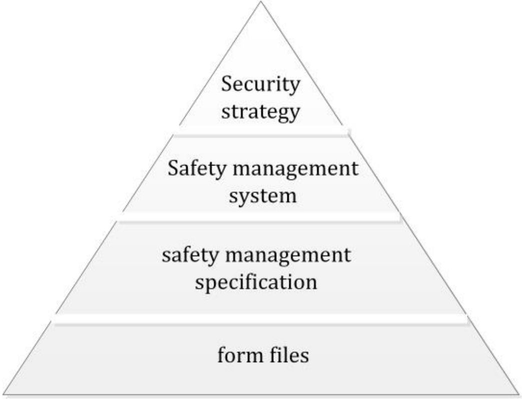

Fig. 4. Data Security Governance Institutional Architecture

On the basis of sorting out data assets, combined with professional classification and application practice, CGS classified all the data assets, monitored and controlled geological data based on classification and security management & control strategies, integrated data security monitoring and protection into the data's full life cycle.

According to the different service scopes and service objects of the geological cloud platform, based on the results of data classification, in accordance with the security requirements of geological data scenarios, and based on authority control, data security management capabilities are embedded into the business process. Along with the implementation of technical management and control, there are basic network protection, system protection, application protection, etc., to jointly ensure the compliance and security of data use. Security auditing realizes the whole process of data usage, timely auditing of user operations, real-time blocking of illegal actions, and timely alarming of risk events.

Through the daily operation and management of geological data, data management personnel carry out data dynamic protection, data backup, education and training, monitor the data flow process in real time, regularly output analysis reports, propose rectification measures, and follow up on the improvement of rectification. During the operation of the geological cloud platform, data managers timely adjust the security strategy, track the implementation of the security management system, and continuously revise the system documents. All units do safety skills training as planned to improve the safety level of data management personnel, so that the safety management ability is on the rise along with the data management operation process.

4 Conclusions and technical outlook

In the process of geological cloud data security management, the security management system, technical system and operation system have been established to effectively ensure the security of geological survey data, realize the free circulation of geological data, and support the work of geological survey business.

Faced with the complexity of data security governance, the data protection system is undergoing continuous technological evolution based on traditional injection or vulnerability attack protection, authentication and access control, encryption, auditing and other technologies, as follows:

1. Scenario-based active prevention and control are incorporated into the data security technology system. For different data protection requirements, the system should determine the appropriate data security protection technical means, break through the traditional one-size-fits-all protection means, and build a dynamic and systematic technical protection framework.
2. In terms of ensuring data security, confidential computing, privacy computing and other implementation scenarios based on cryptographic technology to protect data transactions and share security have been launched [4].
3. Use new technologies such as artificial intelligence (AI) and big data to improve security products and security solutions. Use big data for event mining and auditing, and establish blacklist database as the basis for decision-making of risk control systems to serve access control; use AI to learn, improve security protection rules, and execute auxiliary defenses to improve data security protection [3].

Acknowledgments

This paper is supported by the following projects funding: Second class project of China Geological Survey---Geoscience Data Integration and Services (NO. DD20221785)

References

1. Ministry of Industry and Information Technology, 2022. "14th Five-Year" Big Data Industry Development Plan. https://www.miit.gov.cn/jgsj/ghs/zlygh/art/2022/art_5051b9be5d4740daad48e3b1ad8f728b.html.
2. The Central People's Government of the People's Republic of China, 2020. Opinions of the Central Committee of the Communist Party of China and the State Council on Building a More Perfect Market-Based Allocation System and Mechanism. http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm.
3. Zheng YW. Data Security Architecture Design and Practice. (2022). Machinery Industry Press, Beijing.
4. Data Security Governance Professional Committee of Zhongguancun Network Security and Information Industry Alliance, 2022. Data Security Governance White Paper 4.0.

5. The Central People's Government of the People's Republic of China, 2015. Action Plan for Promoting the Development of Big Data. http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm.
6. UFIDA platform and data intelligence team. (2022). Data governance Strategies, Methods, Tools and Practice. Machinery Industry Press, Beijing.
7. DAMA International. (2022). DAMA Guide to the Data Management Body of Knowledge. China Machine Press. Beijing.
8. GB/T 37988-2019. (2020). Information security technology –Data security capability maturity model.