On Data Classification and Grading Methods for Petrochemical Enterprises

Pingping Zhao[1,a], Tao Zhang[2,b]*, Xiaoman Cheng[1,c], Weiqing Huang[1,d], Zhiqi He[1,e]

[a]zhaopingp@petrochina.com.cn, [*b] Corresponding author: zhangtao@tsinghua-eiri.org, [c]chengxiaoman@petrochina.com.cn, [d]hwq1992@petrochina.com.cn, [e]hezhiqi7@petrochina.com.cn

[1]Digital Intelligence Company PetroChina Southwest Oil & Gasfield Company Chengdu, China
[2]Sichuan Energy Internet Research Institute Tsinghua University Chengdu, China

Abstract—Data classification and grading management is crucial for ensuring data security and facilitating rational development and utilization. Petrochemical enterprises, as custodians and processors of data, urgently need to establish a unified and scientific system for safeguarding classified data. This article proposes a hybrid classification approach that considers multiple dimensions such as the origin, business domain, and security attributes of petrochemical enterprise's data to construct a multi-tiered data classification system. By comprehensively considering the objects, the scope and the extent of impact, the petrochemical enterprise's data is graded into four levels based on their varying degrees of sensitivity.

Keywords-Petrochemical enterprises; Data classification and grading; Data security

1 INTRODUCTION

With the progressive advancement of the industrial Internet, the security of industrial data has exerted a profound impact on contemporary industry, thereby rendering the assurance of data security in the industrial Internet a pivotal strategic imperative for nations. Data security is of paramount importance in China, and a series of pertinent policy documents have been promulgated. According to a notification on guidelines for the enhancement of industrial Internet security issued by ten organs of Chinese government on July 26, 2019, the enhancement of data security protection capability in the industrial internet is imperative, necessitating the formulation of comprehensive requirements for secure safeguarding throughout the entire life cycle encompassing data collection, storage, processing, transfer, and deletion. Enterprises are mandated to enhance their anti-theft and anti-tampering measures pertaining to research and development design, industrial production, operation management, platform knowledge mechanism as well as digital models alongside data backup [1]. After the promulgation of the *Cybersecurity Law of the People's Republic of China* in 2016, data resource security protection is being continuously accelerated in China such as the establishment of a big data management system and the implementation of data classification and grading [2]. The *Data Security*

ICPDI 2023, September 01-03, Chongqing, People's Republic of China
Copyright © 2023 EAI
DOI 10.4108/eai.1-9-2023.2338835

Law of the People's Republic of China was promulgated in 2021 emphasizes the responsibility of all departments, institutions, and enterprises as data security subjects, requires clarification of relevant regulations and requirements to strengthen the classification and grading management of data, enhance data security protection, improve data quality, etc., in order to promote the establishment of a well-organized governance system with scientific classification, accurate grading, and orderly management across different sectors [3].

The security of petrochemical enterprises' data is crucial to personal information, petrochemical sector, regional and even national security. Petrochemical sector data possesses characteristics such as a vast amount, diverse types, and immense potential value; henceforth, its classification and grading are relatively intricate. However, the petrochemical sector has yet to establish a standardized specification for data classification and grading. In practice, challenges remain in terms of inconsistent classification standards between internal and external parties within each enterprise, as well as potential disconnects with the forthcoming important data inventory. Therefore, it is imperative for petrochemical enterprises to develop a scientifically precise data classification and grading methodology that adheres to regulations and standards. This can be achieved by drawing upon the experiences of other sectors and fields while considering their own unique business characteristics. In petrochemical enterprises, data classification and grading are the fundamental work of data security. Through classification and grading, the importance and sensitivity of data are determined, and different types or levels of data correspond to different security policies throughout the data lifecycle, such as collection, transmission, storage, application, and sharing. By classification and grading, petrochemical enterprises can better understand the value and significance of data, facilitate data management and maintenance, improve data management efficiency, and better support decision-making and analysis.

2 CURRENT SITUATION OF DATA CLASSIFICATION AND GRADING IN CHINA

Pilot projects have been initiated in certain rich-in-data sectors and regions to formulate regulations or standards and establish their own data classification and grading protection system [4].

2.1 The Guide on Industrial Data Classification and Grading

The *Data Security Law* mandates that various sectors establish a system for classifying and grading data protection, as well as implementing mechanisms for assessing, reporting, sharing information on data security risks, monitoring and warning, emergency response. Additionally, it requires the establishment of a review system for data security [5]. The classification of industrial data is guided by the *Guide on Industrial Data Classification and Grading (Trial)*, which takes into account the sectoral requirements, business scale, data complexity, and other practical factors. In terms of data grading, the guidelines categorize industrial data into three levels: Level 1, Level 2, and Level 3 based on the

potential impact on industrial production and economic benefits resulting from tampering, destruction, leakage or unauthorized use of different categories of industrial data. Simultaneously, the guidelines also encompass management requirements for safeguarding industrial enterprise data security and emphasize comprehensive life cycle protection measures, with a specific focus on graded protection mandates tailored to different levels of industrial data security. It is advisable for enterprises to maintain consistent data classification and grading practices while fortifying security provisions throughout the entire lifespan of their data [6].

2.2 Government data and public data

The government application data has broad applicability, lengthy processes, high value, and robust protection. However, it faces challenges such as extensive exposure, multiple points of contact, heightened threats, and difficulty in realizing its full potential. While implementing consistent security measures for all data is not enough to meet new requirements, using classified security protection measures enables effective utilization of data for novel production demands and prevents data leakage. This approach achieves fine-grained management of data security [7].

In the realm of government and public data, various regions adopt a multi-level approach to classify their data. Their hybrid classification method is commonly utilized and can be divided into two types: Guizhou and Sichuan Province classify their data based on dimensions such as resource attributes, collection management, security management, sharing, and openness; while Chongqing Municipality and Zhejiang Province classify their data according to dimensions like data subjects, business domains, and security attributes. Each region considers three factors - the objects, scope, and extent of impact - when classifying the data. The former includes national security or the legitimate interests of individuals or organizations. The latter is generally classified into mild, moderate or severe, and typically graded into four levels [8].

2.3 Telecommunication Data

In the telecommunications, data controlled by basic telecommunications enterprises is categorized into two types: user-related and company-owned. The *Data Classification and Grading Method of Basic Telecommunication Enterprises* determines the security level of the data as sensitive, relatively sensitive, low-sensitive, or non-sensitive based on their scope of impact and extent of harm after destruction [9]. The *Practical Guideline for Cybersecurity Standards - Classification and Grading of Cyber Data* issued by the National Information Security Standardization Technical Committee pointed out that data classification encompasses multiple perspectives and dimensions. In terms of facilitating data management and utilization, data can be classified from diverse angles such as geographical location, industry sector, organizational structure, etc. Simultaneously, the data from diverse domains in telecommunications and the Internet will be centrally and coordinately managed and classified into three levels. They will also be graded based on their sensitivity and enterprise expertise [10].

2.4 Electricity Data

In 2022, the article 25 of the *Cybersecurity Management Measures of the Electricity Industry (Revised Draft)* issued by the General Department of the National Energy Administration clearly says that electricity enterprises should establish and enhance a comprehensive data security management system as well as a mechanism for protecting personal information. In accordance with the requirements outlined in national and sectoral important data inventories along with data classification and grading protection, specific inventories of crucial data pertaining to their respective institutions need to be determined, with particular emphasis on safeguarding the listed information [11].

According to the *Measures*, the electricity data can be classified - on its storage types or business attributes - into the structured, semi-structured and unstructured data, or the production, management, marketing, operation, and maintenance data. It is usually classified from two dimensions: the objects and the extent of impact, serving as a foundation for determining the level of data security by assessing the extent to which damage to data security impacts the object. That is to say, the extent of impact on the objects decides the security level of data. The objects of impact mainly refer to national security, public interests, citizens and enterprise's rights and interests while the extent includes five levels from none to severe. Electricity data is divided into four levels through the two-dimensional matrix of objects and extent [12].

Due to the dynamic nature of electricity data, its security level is not static and may fluctuate based on various factors such as significant aggregation, exponential expansion or contraction in scope, or changes in timeliness. As per regulations, it is imperative to reevaluate the security level of data under such circumstances.

2.5 Financial Data

Financial data exhibits significant characteristics of high volume and value, necessitating focused protection on the most sensitive and valuable information within financial datasets. As such, the financial sector places great emphasis on classifying, grading, and securing its data assets. Currently, three standards pertaining to data classification and grading have been released within the financial sector, including the *Financial Data Security - Guidelines for Data Security Classification* (JR/T 0197-2020), the *Data Classification Guidelines for Securities and Futures Industry* (JR/T 0158-2018), and the *Personal Financial Information Protection Technical Specification* (JR/T 0171-2020), with regulations for the classification and grading of financial data, encompassing dimensions such as financial data, securities and futures data, and personal financial information. The *Financial Data Security - Guidelines for Data Security Classification* specifically requires that financial institutions are obligated to adhere to the *Financial Data Security - Guidelines for Data Security Classification* in order to effectively classify and grade their financial data assets, while also exploring the establishment of a mechanism and supporting system for safeguarding the security grading of financial data within their own institution. This initiative aims to facilitate the exchange of financial data among institutions and across sectors. The *Guidelines* offer clear criteria and regulations for the classification of financial data, providing best practices and specific guidance to financial institutions in conducting grading and security assessments of their data. A five-level classification system is established based on the objects and extent of impact caused by

breaches in data security for financial institutions, ranging from high (Level 5) to low (Level 1) levels of data security [13].

3 DATA CLASSIFICATION AND GRADING METHODS OF PETROLCHEMICAL ENTERPRISES

Based on the current state of data classification and grading in various sectors, a combination of line and plane classifications can be adopted to classify petrochemical enterprise data from multiple dimensions, considering factors such as data source (object), business attributes, and security attributes. This approach effectively reflects the characteristics of both business and data while also being compatible with existing data classification systems. The resulting four-level classification system for petrochemical enterprise data is based on comprehensive consideration of the object, the scope, and the extent of impact with respect to the integrity, confidentiality, and availability of data.

3.1 Methods of Data Classification

1) The Methods

Petrochemical data has the characteristics of large amount of data, complex business logic, high degree of data specialization and high degree of data sensitivity. When classifying the data of petrochemical enterprises, there are problems such as difficulty in identifying and combing through data assets, lack of corresponding classification standards and methods, and lack of corresponding data classification technical support [14], so it is key to establish an operable, scientific, standardized, and comprehensive data classification method.

In the *Definition of Common Terms Used in Classification and Coding* (GB/T 10113-2003), there are two fundamental methods of classification: line classification and plane classification. The former involves classifying objects based on selected attributes or features, with multiple levels and categories within each level. This method offers a hierarchical structure that effectively reflects logical relationships between categories but lacks structural flexibility. On the other hand, the latter entails selecting attributes or features to divide objects into independent categories, forming distinct “planes” which can be arranged parallelly based on specific data. It provides greater flexibility compared to line classification [15].

Given the intricate and voluminous nature of petrochemical data, achieving scientific, standardized, and convenient management requires a mixed classification approach that combines line-based classification with supplementary plane-based one. This approach is based on single data attribute dimensions at the same level and different ones at different levels. Specifically, we propose a business-oriented topic domain partitioning method that distinguishes between common data topics and business-specific topics before segmenting the data along “lines”.

The specific steps for classification include 1) identifying data sources, clarifying ownership and access rights for data tracing; 2) based on business attributes, defining application scenarios, assessing value for specific uses and selecting analysis schemes; 3) specifying distribution scenarios and identifying potential industries that could benefit from the available

data types and scope; 4) assessing the quality of available data to determine its suitability for various applications, clarifying any additional requirements needed to support effective use and develop a comprehensive plan for managing all aspects related to ensuring high-quality results; 5) comb through data security attributes, determine data sensitivity and openness

2) The Dimensions

Considering the requirements of current laws and regulations on data security protection, as well as the needs for data classification and grading, a business-oriented approach is adopted to divide the data subject domain into two categories: public data subject domain and business subject domain. Please refer to Figure 1 for the data classification diagram of petrochemical enterprises (taking an oil and gas field company as an example), while specific dimensions of classification are described below.

The first is the public data subject domain. The term "public data" refers to valuable data that can be reused throughout the company, requiring consistency, integrity, and control across different systems (operational / transactional applications and analytical systems). Managing public data separately helps improve corporate data utilization and lays a stronger foundation for integrating corporate information. This domain is divided into two levels based on its categories, with the option for further subdivision up to four levels. For instance, an oilfield company's public data subject domain may include basic data, master equipment data, and oil and gas product classification as level two subjects that can be further subdivided into three levels according to specific needs.

The second is the business subject domain, which is categorized based on the company’s professional fields with each one undertaking a specific area of business with clear boundaries. The divided business subject domains cover all aspects of the company's operations without overlapping or duplicating. For instance, the oil and gas exploration business subject domain can be further subdivided into areas such as oil and gas exploration, oil and gas development, oil engineering technology, and oil and gas distribution. It is essential that the naming accurately reflects the meaning and function of each subject: 1) Based on the division of responsibilities among functional departments and professional companies, including finance, human resources, material supply chain, exploration and production, oil refining and chemical industry, public data and 28 other categories according to CNPC's business structure for operation management and professional management. 2) With each sub-classification independent to avoid interdependence while maintaining a consistent logical structure at the same level. In principle, there should be no more than six levels in total. If there are more than six levels required without changing the first-level subject (business subject domain), then compressing the upper level or re-dividing the level is necessary.

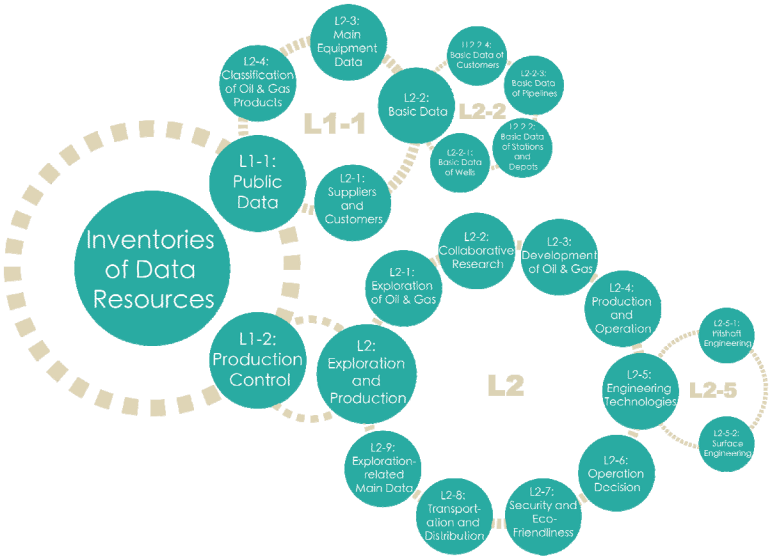

Figure 1. A Data Classification Diagram of Petrochemical Enterprises

3.2 Methods of Data Grading

1) The Elements

In accordance with the *Data Security Law*, it is imperative to develop data classification methodologies that align with industry standards and cater to specific enterprise requirements. The *Law* mandates a hierarchical and categorized approach for safeguarding data based on its significance in economic and social development, as well as the potential risks posed to national security, public interests, or the lawful rights and interests of individuals and organizations when subjected to tampering, destruction, leakage, illegal acquisition, or unauthorized usage.

The *Law* also stipulates that data related to national security, the backbone of the economy, vital livelihoods, and significant public interests are classified as core data of the country and subject to more stringent management systems. Specific inventories of these data within respective industries and fields must be established for priority protection. However, there is currently no consensus on inventories of important data tailored for the petrochemical though they should be identified before classified and graded. Therefore, consideration should be given to both the importance of the data and potential damage caused by its compromise in line with the substantive requirements outlined in the *Law*. Experiences from other industries' systems should be referred to while considering the unique characteristics of petrochemical enterprises. Additionally, a broader scope of impact should be examined when grading petrochemical enterprise data due to its significance as mandated by the *Law*.

Data being graded, it is essential to identify the impacted objects in case of a compromise in data security, followed by an evaluation of the scope and severity of impact on these subjects.

Firstly, the objects impacted by data compromises include national security and public interests, the petrochemical' overall interests, enterprise's interests, and individual interests. In terms of national security and public interests, compromised data security attributes (integrity, confidentiality, availability) may affect the order of economic activity and production operation related to national security and public interests. Concerning overall interests of the petrochemical, they may affect the order within one or more enterprises in the sector [16]. Regarding an enterprise's own interests, they may affect the social rights and economic benefits of the company as well as its juridical person or internal departments. Finally, the last one refers to general information or privacy of an individual.

Secondly, the scope of impact encompasses multiple sectors, multiple enterprises within one sector, the enterprise itself, as well as its secondary and tertiary bodies. When assessing the extent of impact, the scope plays a significant role in determining the controllability of data destruction. In cases involving substantial data volume and wide-ranging consequences such as numerous customers, significant financial resources or clients from multiple sectors and institutions, a high extent of impact should be assigned. Damage of different types of data result in varying levels of harm to different stakeholders' interests; thus, determining the sensitivity level for data security becomes essential. The evaluation of data sensitivity level should be based on identifying whose interests are most severely affected.

Thirdly, the extent of impact is a qualitative measure used to describe the effects of an event. It cannot be quantitatively measured without actual occurrences and their resulting consequences. Even in practical scenarios, it remains challenging to accurately quantify the direct and indirect implications caused by various events and accidents. However, by integrating enterprise standards such as the *Specification for the Emergency Response to Information Security Incidents* (Q/SY 10345-2020) and considering the characteristics of the data type, it becomes possible to determine the extent of impact.

Furthermore, the combination of multiple-field data can potentially reveal various pieces of information due to data correlation. In this scenario, it is crucial to adhere to the principle of prioritizing higher-level data over lower-level ones and assign a grading based on the data level that is most severely affected by potential data damage. Additionally, consideration should be given to the timeliness of the data, and after a certain period, its grading can be considered as relatively low.

2) The Standards

According to the business domains and data application scenarios across various industries, a three-tiered grading approach, the core data, the important data, and the common data is currently proposed in the *Guide on Industrial Data Classification and Grading (Trial)*. Based on a company's ownership, utilization, and processing of its data, it can be further graded into four levels considering its suitability for public disclosure. The higher the level, the more severe the impact of damage will be on the data; overcoming challenges and eliminating costs will also become more demanding; moreover, its effects will persist longer and have a broader scope.

Data grading is generally performed in the following four steps: First, determine the objects that may be impacted after the security attributes (integrity, confidentiality, availability) of a certain type of data to be graded are breached, including national

security and public interests, the overall interests of the petrochemical sector, the enterprise's interests, and the individual interests; Second, determine the scope that may be impacted, including multiple sectors, multiple enterprises within the sector, the enterprise itself, and its secondary and tertiary bodies. Third, determine the extent of the possible impact, including severe damage, serious damage, and general damage; Fourth, based on the above steps, grade the object, the scope, and the extent of impact.

In formulating specific grading standards, the determination of data security grades should be comprehensive and considerate of their impact on individuals, enterprises, sectors, the society, and the nation. Personal information-related data should be graded according to the *Information Security Technology - Guidance for Personal Information Security Impact Assessment*, referring to Table 1.

TABLE 1 THE SCHEMATIC TABLE OF DATA GRADING RULES

Objects of Impact	Scope of Impact	Extent of Impact	Importance Level	Grade of Data
National Security and Public Interests	Multiple Sectors	Severe	Top	4
National Security and Public Interests	Multiple Enterprises within the Sector	Serious	Top	4
Petrochemical's Overall Interests	Multiple Enterprises within the Sector	Severe	Top	4
Petrochemical's Overall Interests	The Enterprise Itself	Serious	High	3
Petrochemical's Overall Interests	The Enterprise Itself	General	Medium	2
Enterprise's Interest	The Enterprise Itself	Severe	Top	4
Enterprise's Interest	The Enterprise Itself	Serious	High	3
Enterprise's Interest	The Enterprise Itself	General	Medium	2
Enterprise's Interest	Secondary Bodies	Severe	High	3
Enterprise's Interest	Secondary Bodies	Serious	Medium	2
Enterprise's Interest	Tertiary Bodies	Serious	Medium	2
Enterprise's Interest	Secondary and Tertiary Bodies	General	Low	1
Individual Interest	The Enterprise Itself	Serious	Medium	2
Individual Interest	The Enterprise Itself	General	Low	1
Individual Interest	Secondary and Tertiary Bodies	Serious	Low	1

3.3 Workflows of Data Classification and Grading

1) The Organizational Framework

The organizational framework for data classification and grading should clearly delineate the management bodies, designate the highest accountable individual, specify roles and functions, as well as establish an authorization mechanism.

2) The Management System

The successful implementation of data classification and grading requires institutional

support, including specifying requirements, delineating roles, and responsibilities, establishing mechanisms for policy development and maintenance, devising performance evaluation mechanisms, outlining daily management processes, providing operational guidelines for personnel involved in this undertaking. It also involves principles and methodologies for data categorization and alterations in data levels as well as notification protocols subsequent to modifications. Furthermore, it entails periodic review of the classified resource inventory based on established principles and formulation of overarching objectives for safeguarding classified information.

Petrochemical enterprises should establish a comprehensive system of data classification and grading regulations to effectively guide and coordinate the implementation of this work. Each competent department bears the responsibility for promoting internal data classification and grading within the company. The company assumes primary accountability for data management, necessitating robust systems that encompass data classification, grading, annual reviews, as well as timely updates in response to significant changes in company systems or operations. Considering actual needs, it may be advisable for the company to establish a dedicated entity staffed with specialized personnel for managing data.

Petrochemical enterprises should follow the *Guidelines for Information Security Protection of Industrial Control Systems* (issued by the Ministry of Industry and Information Technology in October 2016) while considering data classification to ensure appropriate safeguarding measures. In case of tampering, destruction, leakage, or unauthorized use of industrial data, companies must promptly execute emergency response procedures according to their pre-established contingency plans.

3) The Workflow

The data classification and grading process consists of three stages, as shown in Figure 2. Firstly, domain subdivision is conducted to address business classification issues and determine the data source, as well as the entity responsible for data management. Identifying the accountable entity ensures accurate data classification and grading. Secondly, data classification should be focuses after clearly identifying the responsible entity and business classification. Then it is recommended to specify the 'forms of data' including its system environment, storage medium, physical location, etc. Lastly, data is graded based on the results of its classification.

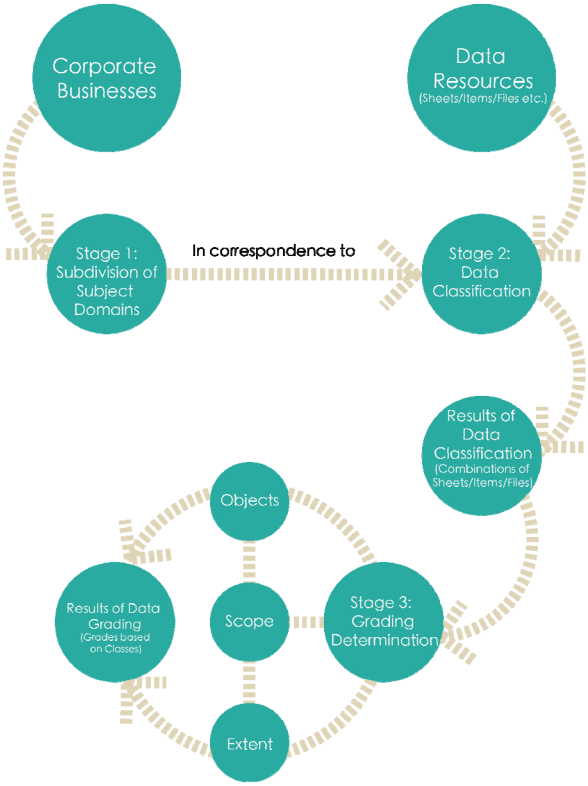

Figure 2. A Basic Workflow of Data Classification and Grading

The implementation of data classification and grading should be facilitated by software tools, utilizing customized software with techniques such as labeling for batch data classification and grading. This approach can minimize the manual intervention and enhance the efficiency.

4 Conclusion

With the introduction and implementation of the *Data Security Law* and the *Personal Information Protection Law*, data security is now strictly regulated. Petrochemical enterprises should establish a robust end-to-end data security management system [17] in compliance with legal requirements. Data classification and grading management are essential for strengthening data exchange and sharing, enhancing the value of data resources, and effectively governing data security. Currently, ensuring data security governance poses challenges. However, standards such as *Guidelines for Information Security Protection of Industrial Control Systems* and the *Guide on Industrial Data Classification and Grading (Trial)* have prompted petrochemical enterprises to focus on improving their data management capabilities while reinforcing guarantees for data

security. In future endeavors, refined unified scientific methods and standards will be established through pilot projects across various subs within this sector. This article presents the author's initial investigation into classifying and grading data projects in the petroleum and natural gas enterprises. Methods, tools, systems, and processes associated with classification and grading will be further explored to facilitate the establishment of a data classification and grading ecosystem for oil and gas enterprises, as well as to foster consensus on data classification and grading governance in the petrochemical sector.

Acknowledgments. Supported by the National Key Research and Development Program of China (2020YFB1710000).

REFERENCES

[1] Y. Li, Status Quo and Development of Data Classification and Grading [J], China Information Security. 2021(5): pp.55-56.

[2] Standing Committee of the National People's Congress of the People's Republic of China, The Cybersecurity Law of the People's Republic of China [EB/OL], Nov.7 2016, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[3] X. Shang and H. Han, Systematic Construction of Data Classification and Grading Governance Norms [J], E-Government, 2022(10): pp.75-87.

[4] S. Li and Z. Xie, Analyses on Data Classification/Grading and Relevent Standards [J], China Quality and Standards Review, 2019(4): pp.14-16.

[5] Standing Committee of the National People's Congress of the People's Republic of China, The Data Security Law of the People's Republic of China [EB/OL], Jun.10 2021, http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm.

[6] Lowry L .Bridging the Business Data Divide: Insights into Primary and Secondary Data Use by Business Researchers[J].IASSIST quarterly / International Association for Social Science Information Service and Technology, 2015, 39(2):14.DOI:10.29173/iq779.

[7] L. Hou and S. He, How to Protect Data through Classification and Grading [J], Procecutorial View, 2020, 28(19): pp 14-15.

[8] Administration for Market Regulation of Guizhou Province, DB52/T 1123-2016, Govemental Data - Guidelines for Categorization and Classification of Data [S], Guizhou: Administration for Market Regulation of Guizhou Province, 2016.

[9] China Communications Standards Association, YD/T 3813-2020, Data Classification and Grading Method of Basic Telecommunication Enterprises [S], Beijing: China Communications Standards Association, 2020.

[10] National Information Security Standardization Technical Committee, TC260-PG-20212A, Practical Guideline for Cybersecurity Standards - Classification and Grading of Cyber Data [S], Beijing: National Information Security Standardization Technical Committee, 2021.

[11] Z. Yang and Z. Wang, Recommendations for the Security of Industrial Data for Industrial Enterprises [J], The Journal of New Industrialization, 2021,11(10): pp.141-143.

[12] S. Ling, Y. Song and K. Liu, On the Methods of Data Classification and Grading for Electricity Enterprises [J], Management and Technology of SME, 2023(01): pp.109-111.

[13] National Financial Standardization Technical Committee, JR/T 0197-2020, Financial Data Security - Guidelines for Data Security Classification [S], Beijing: National Financial Standardization Technical Committee, 2020.
[14] Correia A , Gua P B .A holistic perspective on Data Governance[C]//CORPORATE GOVERNANCE: A SEARCH FOR EMERGING TRENDS IN THE PANDEMIC TIMES.2021.DOI:10.22495/cgsetpt12.
[15] J. Chen, T. Wang, Q. Wang and Etc., On the Paths of Enterprises Data Classification and Grading [J], Network Security Technology & Application, 2022(4): pp.70-71.
[16] Deverka P A , Majumder M A , Villanueva A G ,et al.Creating a data resource: what will it take to build a medical information commons?[J].Genome Medicine, 2017, 9(1):84.DOI:10.1186/s13073-017-0476-3.
[17] Standing Committee of the National People's Congress of the People's Republic of China, The Personal Information Protection Law of the People's Republic of China [EB/OL], Aug.20 2021, http://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm.