

Apply the principles and practices of Data security, Governance and Compliance based on a given scenario

Huazhi Lin
2200376
(of Affiliation)
Software Engineering and Artificial
Intelligence program
2200376@student.uwtsd.ac.uk

Abstract—Information has evolved into a key resource in the enterprise market competition in the age of economic globalization and the Internet. The organization faces a variety of information security concerns as it digitizes. Several information security standards have also been released, and international theoretical research on information security is a rapidly growing and expanding study direction. This essay examines several information security models first, using CoffeeBlend as an illustration, then applies the theory of information security management to the company's actual problem analysis and development of a solution before putting out a risk management strategy.

Keywords—information safety, security model, risk assessment

I. INTRODUCTION

The worldwide social and economic organization structure is shifting from energy and material to knowledge and information technology in recent years due to the rapid development of Internet information technology. Enterprises frequently use information systems, and it is well-understood how important information is. wide acceptance. Modern businesses typically store important data in network data centers, including operational information, marketing strategies, and consumer information. Additionally, a variety of information systems are inextricably linked to the data storage in financial reports, employee wages, and personnel files. It is evident that information technology has been applied to every element of business operations and management, and that information itself has grown to be a significant intangible asset for the business.

Enterprises are not just dealing with threats to their information security while benefiting from information technology. Network security incidents involving both domestic and foreign businesses have become commonplace in recent years. These incidents include common DDoS denial-of-service attacks, remote command execution, sensitive data leakage, webpage tampering, Trojan horse viruses, etc., like the "WannaCry" ransomware that affected the entire world in 2017. Unpredictable losses resulted from the infection of hundreds of thousands of hosts across numerous locations and the permanent loss of enormous amounts of data [1]. Enterprise information security events accounted for 35.6% of data leakage occurrences in 2020, according to data from the National Industrial Information Security Strategy Development Research Center, indicating a consistently increasing trend over the previous three years as seen in Figure 1.

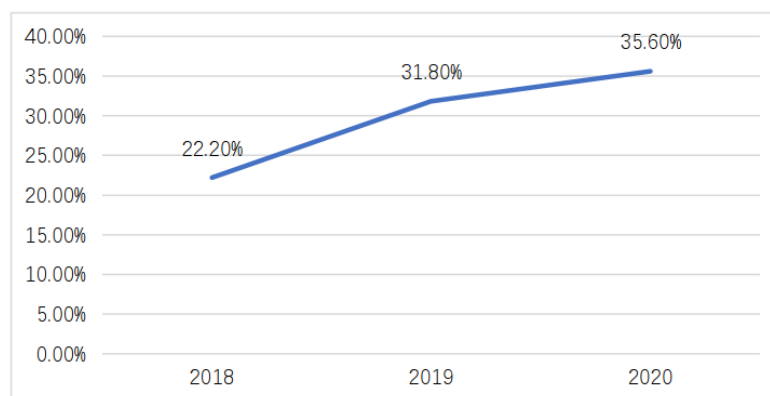


Fig. 1. percentage of data breaches in worldwide corporate information security incidents from 2018 to 2020.

Enterprises gradually tend to improve enterprise management efficiency through industrial informationization to strengthen their core business capabilities and better adapt to the constantly changing domestic and international markets. However, when building an enterprise's digital infrastructure, businesses frequently focus primarily on the convenience that digitization brings to managing their employees and business processes, oblivious to the inherent risks that come with inadequate information protection. Enterprise development may suffer unfathomable costs if the information security risk cannot be appropriately controlled.

II. INFORMATION SECURITY MODEL

As information and data security disciplines mature, more security models are being produced. The research on each security model is listed below.

A. ITIL

The British National Computer Bureau first proposed the ITIL (Information Technology Infrastructure Library) series of service management standard libraries in the 1980s to address the real-world issues associated with "poor IT service quality." The use of (IT) applications is also a way for businesses to efficiently manage the design, development, deployment, and use of IT information systems. It also teaches us how to better maintain and manage IT services [2]. The traditional IT management system places a strong emphasis on technology, in contrast to the IT theoretical framework, whose management system is process-based, customer- and service-oriented. The transition from the conventional passive technology-supported management technique to the service-centered active service method is finished through the transformation of process-oriented service. Figure 2 illustrates ITIL's core architecture.

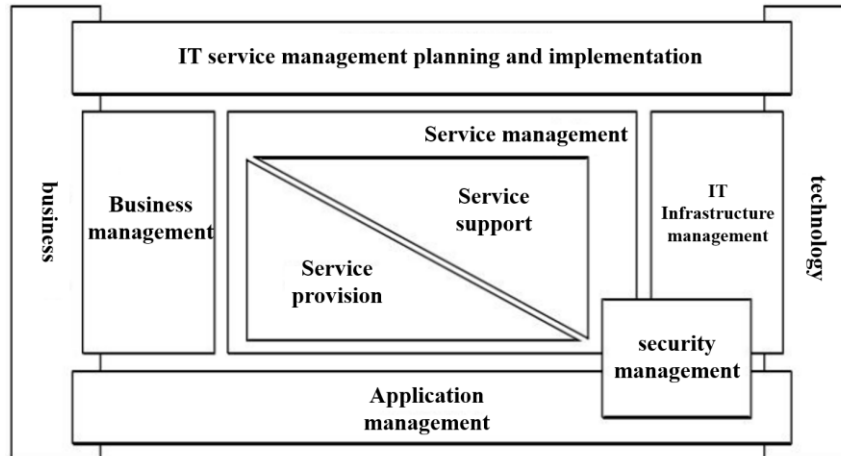


Fig. 2. ITIL main frame diagram

The business management, IT infrastructure management, application management, planning and implementation of IT services, security management, and service management modules in IT service management, along with 4 functions and 26 processes, are all depicted in the ITIL main frame diagram. The service management module serves as the framework's central component, and other modules rely on it to communicate with one another. Together, these modules make up the ITIL main framework. There are two categories of service management: support and provision, which handle the content and procedure of IT services, respectively. It primarily consists of 10 core processes and service desk operations.

In the context of service management, the service provision group primarily oversees the supply of IT services, including service level management, service capability management, availability management, financial management about IT services, and continuity management. The service support group in service management is primarily responsible for overseeing the administrative procedure for users to acquire IT services, which encompasses several essential procedures such as service desk activities and events, changes, issues, configurations, and releases.

The main goal of the initial ITIL management framework is to raise the standard of IT service management by constructing IT service departments with standardized procedures. With the release of ITIL V3, it is suggested that functions and processes be reorganized with business as the core, made service-oriented, and built around the actual business of the enterprise using the "service strategy, service design, service introduction, service operation, and service life cycle management" five-ring theory. ITIL is now a methodology and practice manual for IT service management on a worldwide scale thanks to the transformation of the core notion.

B. ISO27000

The second section of BS 7799 is the forerunner to ISO 27001 [3]. The British Department of Trade and Industry drafted BS7799, which the British Standards Institution (BSI) released in 1995. To date, BS7799 has made available three sections. Information security management best practices are mostly covered in the first section, "Information Security Management Implementation Rules." The family of ISO/IEC 27000 series standards keeps expanding. More than 20 standards, including 27000, 27001, 27002, 27003, and 27005, have been published so far, and an additional ten standards are in the process of being created. Currently, many organizations throughout the world adopt and apply the ISO/IEC 27000 series of standards as a set of general safety guidelines. It mostly entails the following seven key steps:

- (1) Preparatory work: identify the team members for the information security management system's creation and specify the timeframe for its construction; gather background information about the organization, the current situation, and the features of the information system;
- (2) Risk assessment: create a plan for risk assessment, carry out surveys and interviews by the plan, gather asset data, assess existing threats and weak areas, and identify risks;
- (3) Conduct a thorough examination of the risk assessment results to identify the breadth of the information security management system's controls;
- (4) Risk management and the creation of an information security system: Create an information security management system framework by the ISO27001 standard, design a new information security management process, and enhance the currently inadequate information security management process;
- (5) Internal audit and management review: Internal audit staff and pertinent high-level staff carry out internal audit assessments and promptly address any flaws discovered;
- (6) Review and approval: External reviewers evaluate and certify the organization's information security management system;
- (7) Continuous improvement: Repeat this procedure as needed to address brand-new information security management challenges while the information security management system is in use;

The information security management system is a cyclical process that adheres to the Deming cycle, as can be seen from the ISO27000 information item security management system standard method, as depicted in Figure 3. At the same time, it is evident that risk assessment and risk control are the primary components of the ISO27000 standard system and have been since the inception of the information security management system. They must be performed not only at the start of an enterprise but also repeatedly and periodically.

C. P2DR2

The P2DR2 security model constructs a dynamic network security theoretical model based on closed-loop control and active defense from the information security strategy, information security protection measures, information security detection methods, information security event response methods, and information security recovery aspects. The quality of the corresponding operators, their technical proficiency, and their method of operation are the key components for the model system to operate normally in its actual implementation.

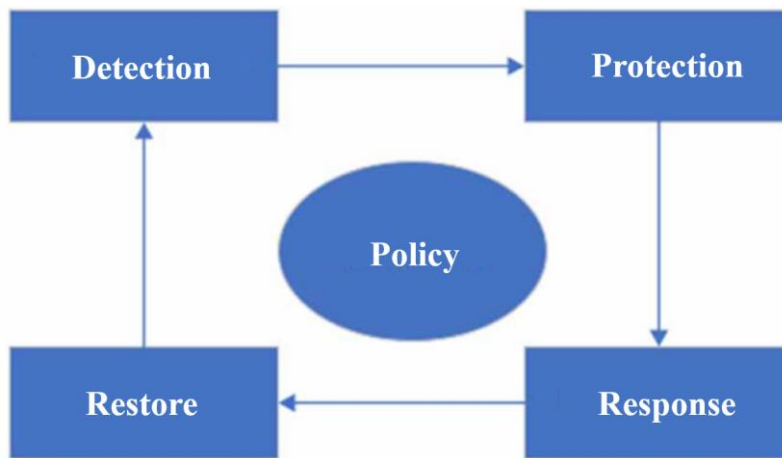


Fig. 3. Schematic diagram of the P2DR2 security model

This model establishes and evaluates network routing and security policies to secure enterprise network interaction. Building a multi-level, all-encompassing, and three-dimensional regional network security environment requires establishing a real-time monitoring and auditing mechanism both inside and outside the network, adopting real-time and dynamic corresponding security measures, and using various techniques like system disaster backup and recovery, key system redundancy design, etc.

III. CURRENT ISSUES AND STUDY OF THE SAFETY MANAGEMENT SYSTEM AT COFFEEBLEND

A. CoffeeBlend Company Introduction

One of the best and most sought-after blends in the world, Jamaican coffee, is offered for sale by CoffeeBlend. CoffeeBlend is widely present throughout the world. To provide IT services to its employees and customers, the business leverages cloud services. Nearly 95% of the company's network, according to estimates, is wireless. Additionally, the business has a sizable web and social media presence to advertise its activities

B. Problems with CoffeeBlend

The company has recently faced intense pressure to let both its personnel and customers utilize their devices to access the company's network and resources due to its sizable staff and multinational customer base. The company's top priority is the security of the personal data of its employees and clients. The business is also worried about safeguarding its priceless intellectual property. The corporation places a high focus on information security, but things are chaotic. Their security requirements are not covered by any recognized policies.

C. Analysis of CoffeeBlend Information Security Management Issues

The reorganization of the organizational structure is the primary reason for CoffeeBlend's information security management issues. However, since CoffeeBlend's founding, there hasn't been a well-developed idea or process for managing information security risk, and there hasn't been a good system in place for effective risk analysis, management, or assessment. Plan of control [4]. As a result, the CoffeeBlend information system requires information security risk management.

(1) Identify the assets and evaluate their significance

Information or resources that can be used by businesses or departments are referred to as assets associated with information systems. These assets are also the intended targets of information system security measures. To ensure the ongoing and reliable operation of CoffeeBlend, the supporting hardware infrastructure, software environment, management of systems, and staff associated with the information system are all company assets. They are also significant items for risk assessment. The degree of harm caused by an information system assault or destruction depends on how these assets' value has changed for the organization or department.

It is required to further confirm the significance of these assets, classify them, and assign values to them after the asset information for this risk assessment has been verified. The influence of the three properties of asset availability, integrity, and confidentiality on business is what determines the importance level of assets. Assignment size can be divided into five assignment levels from 1 to 5, the higher the level, the greater its impact.

(2) Recognize and evaluate dangers

The threat is the probability that a company or organization's utilized resources would result in unanticipated mishaps and harm to the company or organization's interests or safety. The identification of threats to information system assets necessitates a risk assessment process to confirm the threats that may cause potential risks to its assets and analyze the likelihood of their occurrence. This is done to guarantee the continuous and stable operation of the CoffeeBlend information system and ensure that business operations are unaffected. Understanding the present CoffeeBlend information system's asset threats in multiple dimensions.

(3) Evaluate the current risk controls

It is vital to assess the present in-place risk control measures after analyzing the asset information, asset threat, and asset vulnerability connected to the CoffeeBlend information system. The main goals of doing this can be broken down into two categories: First, determine whether the current information security risk management methods are effective to guarantee the stable operation of the CoffeeBlend information system. To prevent resource waste, effective management practices will be maintained and the corresponding management practices won't be rescheduled; second, confirm the weaknesses in CoffeeBlend's information security risk management and determine which components of the management practices need to be changed, corrected, or improved. To fulfill the goal of creating a comprehensive risk management system

Following a thorough evaluation and study of the CoffeeBlend information system's risk issues, the following significant dangers and justifications for the current CoffeeBlend information system are outlined:

(1) There are some flaws in the information security management system. The lack of a unified information security management system across the organization as a result of the in-depth discussion on the company's information security management system had a substantial influence on the group's business operations.

(2) Employee responsibilities are unclear. The job content and breadth of each department's personnel have evolved in tandem with the numerous splits and reorganizations that various functional departments have experienced. Some employees did not finish the handover of work material during the organizational transformation procedure.

(3) Employees do not receive adequate information security training. CoffeeBlend lacks a defined approach for information security training. The top executives of the business concentrate mostly on the project and operation activities that support the group's business operations

There is no comprehensive information security training available for employees since managers have not shown interest in the subject of security management. Employees' lack of awareness of information security management and protection, as well as the frequency of information security events, are directly related to this issue. This has a significant impact on the ongoing and stable operation of the company.

IV. COFFEEBLEND INFORMATION SECURITY MANAGEMENT OPTIMIZATION PLAN

A. Information Security Policy Optimization

(1) Create a file system design for information security

The development of a solid information security management system is essential for the achievement of the organization's information security objectives and a crucial safeguard for the timely and effective progress of information security activity. To create the file structure for the company's information security management system, refer to the ISO27000 safety management system standard. Divide the file system into a four-layer pyramidal structure, with the order being the top layer and the information security policy guidebook as the top-level document. The development of the company's internal safety management system is guided by the overall management program. By outlining the primary system strategies and control points for each control field of information security management, the second-level document will further clarify the overall policy. Technical standards and safety system specifications make up the third tier of documentation. Specific operating procedures, checklists, implementation rules, and other operational guidance manuals, which serve as manuals of instruction for security implementers, make up the fourth tier of documentation. In Figure 4, its architecture is displayed.

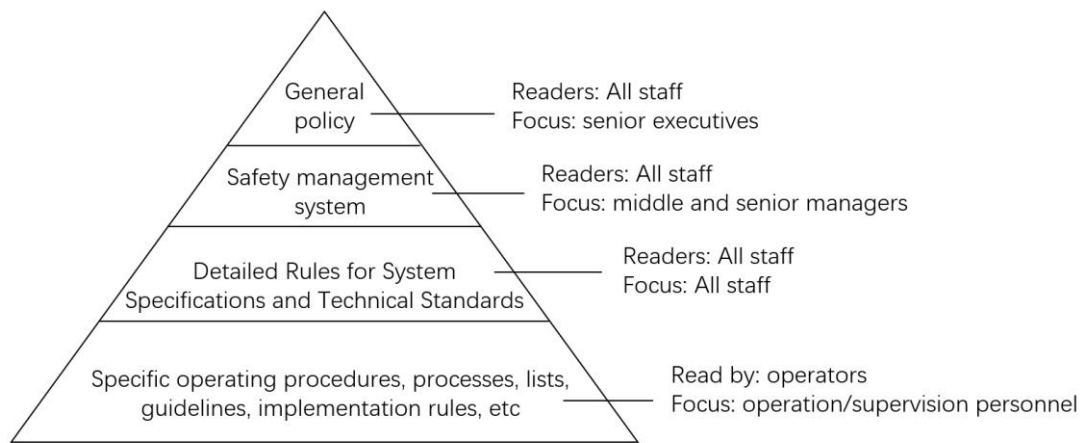


Fig. 4. File structure of information security system

(2) Establish a sustainable improvement system

Information security management is a process that can be enhanced through time. It adheres to the PDCA continuous improvement management model. The theoretical framework for establishing and improving the information security management system in the ISO27000 standard is PDCA. through design, implementation, and examination of the effects of implementation, maintenance, and improvement After completing the P-D-C-A cycle iteration, the firm can transform the specific information security goals and needs into a manageable and controllable information security management system through the process of managing the company's information security. Create a sustainable improvement information security management system for CoffeeBlend using the PDCA cycle model as the guiding theory. In Figure 5, the PDCA management paradigm is displayed.

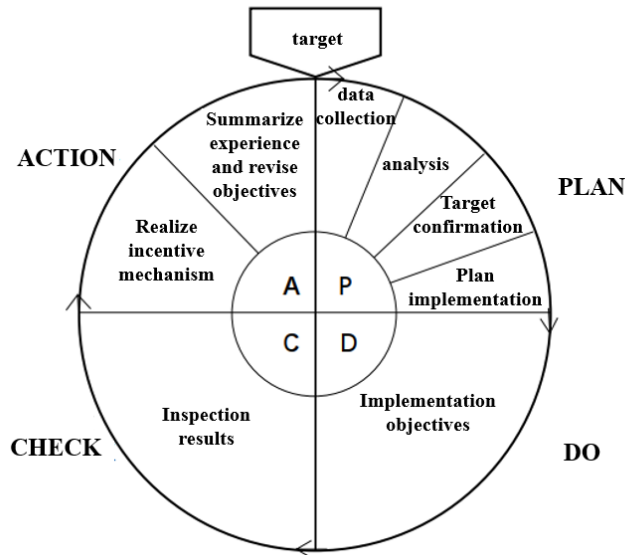


Fig. 5. PDCA management model

B. Improvement of personnel information security

People are both the cornerstone of management and its greatest challenge. Any management system or system cannot be implemented without the involvement of people [5]. All company employees should be fully aware of the significance of information security, improve their level of information security awareness, and become familiar with and follow the company's information security policies and procedures to effectively implement information security control measures. To achieve the goal of improving employee information security quality generally, several human resource sub-modules, including enterprise security culture, training mechanisms, and assessment mechanisms, are thoroughly optimized in this paper using the definition of human resources security management implementation guidelines in the ISO27000 information security management standard.

(1) Information security control before and following employee appointments

The Human Resources Department conducts background investigations and qualification verifications on prospective workers before entry, which includes an information security evaluation. Take information security awareness training and a look at the company's information security system as the main topics of new employee induction training after signing the necessary contracts and information security confidentiality agreements with them to clarify confidentiality obligations and responsibilities

(2) Supporting corporate information security practices

A security notion ingrained in the human brain is security awareness. Employees at the organization can develop an understanding of information security and appreciate its significance by enhancing the promotion of an information security culture. Extrapolate information from previous security events, frequently distribute information security promotional emails via the internal mail system, create security field promotional videos that cover various levels, and utilize animation and interactive techniques to boost involvement; create a knowledge column about information security for the organization's internal forum Expand coverage and acceptance of information security and carry out broad publicity and implementation efforts to integrate information security into the company culture. Publicize information security and carry out information security culture publicity and implementation in a variety of methods

(3) Establishing a platform for information security training

The impact of their knowledge and awareness of information security on the company's internal information security increases with the importance of the job held inside the organization. As a result, there are significant variances in the information security needs depending on an employee's cultural background, technical proficiency, job position, and nature, necessitating the development of suitable information security training programs. The information security training material for CoffeeBlend staff is displayed in Table 1.

Table. 1. Contents of information security training

Type	Trainers	training content	training purpose
Consciousness	All employees of the company	Information Security Awareness Standards and Regulations Policies and Procedures Roles and Responsibilities	Give employees a basic understanding of information security, explain its significance to the business, what policies and procedures must be followed and implemented, what actions at work and in

			personal life will effect information security, and what jobs have security obligations.
Technology	security professionals System R&D staff Operation and maintenance personnel System administrator network administrator	Information Security Core Knowledge System Application systems, security systems and tools technical controls Safety plan and risk control means Authentication and Identification Company Information Security Policies and Procedures	Develop a strong understanding of information security, be able to recognize security risks in information systems with accuracy, eliminate or implement controls, master the fundamentals of information security, comprehend the company's security system, be able to recognize and analyze the fundamental security needs of the business, and seek security solutions.
Management	Senior leadership technical manager Head of Business Unit Business System Leader internal audit staff HR manager	Information Security Core Knowledge System Risk Management and Control System Lifecycle Security Controls Information Security Standards Company Information Security Policy and System Information Security Performance Evaluation Standards	knowing the fundamentals of security management systems and information security-related standards grasp the techniques for reviewing information security system strategies, master the concepts and procedures for organizing, carrying out, monitoring, and enhancing business information security, learn how to evaluate information security performance, comprehend the importance of information security management, and be able to play each function in information security.

C. Optimization of information asset management

Information assets are information resources that a business owns or manages and which may be useful for its operations in the future. To implement effective protection of enterprise information assets, it is first necessary to ascertain which information assets the business currently owns, list the asset catalog, identify which information assets need to be protected, and implement appropriate hierarchical protection by the importance and risk level of information assets. Finally, it is necessary to reasonably define information assets' ownership and protection responsibilities. The hierarchical protection of assets, asset security duties, and processes, etc., for CoffeeBlend's information assets, are all lacking. The following is directed at these two components and is based on the ISO27001 information security management standard's asset management implementation instructions. Optimize information assets' security capabilities from the management's point of view.

(1) Information asset hierarchy management

Information security management requires the hierarchical management of information assets. A technical support system, an internal management system, and a sensible allocation of the time and effort of operation and maintenance employees in the system management process are all built on the classification of information assets. Implement corresponding security protection levels by the various information asset levels at the same time. The classification of documents in the asset list indicates that they are data assets due to the non-standard management of CoffeeBlend documents, and the current document management measures should be reorganized by the level definition of the aforementioned data services, with a reasonable level of confidentiality. Define the security level, organize and put into place the necessary access control permissions, such as the confidentiality levels for the core technical documents that

were exposed during the incursion. Access to data necessitates further permission management. Even if unauthorized access is gained to the laptops of regular employees, no serious information leakage incidents will result.

(2) Determining the roles and procedures for asset management

It is required to organize the asset management process, specify ownership and management duties for information assets, operational methods, and specifications, etc., after adequately classifying and grading them. The responsibility can only be delegated to an individual after the obligations for asset ownership and management are clear. The person in charge of assets is responsible for carrying out asset management tasks and putting the management process in place[6]. The following actions must be performed to increase asset security management due to the lack of asset management security responsibilities, methods, and operating specifications identified in the analysis of CoffeeBlend information asset management security management issues: The service leader for online business services should be in the company's service department. The importance level of services is precisely established on the management platform, and the service support system is logically planned and changed by the importance level of services. To ensure that service assets can achieve the desired availability for high-availability level services, disaster recovery and asset backup procedures, multi-point access, and other steps should be implemented as needed to strengthen the business's disaster recovery capability. The person in charge of the service shall assume the associated security responsibility for the port access privileges of the combing service due to the non-standard management of the CoffeeBlend service port. There are presently just two types of data identified for the data generated or collected by the CoffeeBlend online service: data owners and data administrators. To control access lists and execute routine security risk assessments, corresponding security administrators should be designated. To guarantee the security of data assets, check and confirm the security of data and equipment, etc.

V. CONCLUSION

CoffeeBlend is used as the study object in this paper. After investigating and summarizing the various security models now in use, it focuses on the state of CoffeeBlend's information security management and uses the ISO27000 standard as a framework to conduct risk analysis and examine the causes of the management's issues. develop a corresponding optimization strategy

REFERENCES

- [1] Shen Changxiang. New Opportunities and Network Security in the Era of Digital Economy [J]. Internet Economy, 2019, (4): 94-97.
- [2] Dayal Rasbihari,Vijayakumar V.,Kushwaha Rahul Chandra,Kumar Abhishek,Ambeth Kumar V. D.,Kumar Ankit,Varadarajan Vijayakumar,Kommers Piet,Piuri Vincenzo,Subramaniaswamy V.. A cognitive model for adopting ITIL framework to improve IT services in Indian IT industries[J]. Journal of Intelligent & Fuzzy Systems,2020,39(6).
- [3] Ines Meriah,Latifa Ben Arfa Rabai. Comparative Study of Ontologies Based ISO 27000 Series Security Standards[J]. Procedia Computer Science,2019,160(C).
- [4] Saleh M S, Alfantookh A. A new comprehensive framework for enterprise information security risk management[J]. Applied computing and informatics, 2011, 9(2): 107-118.
- [5] Kobis Pawel. Human Factor Aspects in Information Security Management in the Traditional IT and Cloud Computing Models[J].Operations Research and Decisions,2021,31(1).
- [6] Li Xinhai. Y Company Information Security Management Optimization Research [D]. Guangxi Normal University, 2022. DOI: 10.27036/d.cnki.ggxsu.2022.000616.