

Research and Application Based on Data Security Model

Zheming Zhang (2106318)

Research and Application Based on Data Security Model

Abstract

The growing severity of the information security problem has shifted the focus of human society to the subject of information security. Policies and regulations, the external environment, management systems, and other factors all have a role in information system security, which is difficult to solve entirely by technical means. The construction of an information security management system will become an effective means of reducing information security risks in order to cope with and avoid the increasingly critical information security challenges. Certification can help to demonstrate the information security management system's efficacy, sufficiency, and professionalism.

1.Introduction

1.1Information security

Because information is so valuable, organizations must take great care to ensure its security. The loss of critical information will directly result in the enterprise's interests being lost, and protecting information is to defend the enterprise's interests. In the current era, data is referred to as "gold" or "oil," and it is quickly becoming a major asset for businesses, a source of innovation, and a strategic resource for the country. Data is getting increasingly valuable, so it's no surprise that it's become a prime target for crooks. They not only steal data for resale, but

they also utilize extensive data to develop accurate fraud operations, and they even encrypt user data and then demand a ransom, which has become one of the most common attacks today. Computers and networks are widely employed in modern businesses, and the regular running of businesses is inextricably linked to the normal operation of information systems. Maintaining the usual operation of the business means keeping the information system up and running. Information and information systems are also the competitiveness and productivity of businesses, and protecting them is the best way to protect businesses' competitiveness and productivity. Enterprises must examine the issue of preserving the security of their own information assets to avoid data loss. As a result, numerous firms are paying increasing attention to information security protection.

1.2 Current State of Enterprise Information Security Management

1.2.1 Technical issues

In Information Security Application security, data security, host security, network security, security audit, and security management are all aspects of information security. Due to technology restrictions and capital expenditure constraints, faults and vulnerabilities in the design and development process of company information systems are unavoidable, resulting in concealed threats to enterprise information security. Furthermore, businesses have not formed professional departments or teams to design, operate, and update enterprise information systems, and some businesses lack expert IT security management employees,

resulting in a high number of data security incidents.

1.2.2 Information security management issues

(1) Inadequate overall planning Businesses fail to develop long-term information security management plans that are tailored to their specific requirements. Company executives are unable to successfully provide guidance and development directions because they have limited engagement in information security planning or because their professional competencies are restricted. Enterprises will face information security crises due to issues such as imprecise security objectives, ambiguous management duties, and uncontrolled key information assets.

(2) There is no information security management system in place. Because information security is a relatively new industry, the government's information security rules and regulations are not faultless, and the punishment and control scope are insufficient to fulfill contemporary corporate security requirements. Most businesses have yet to develop an information security management system that is tailored to their specific needs, resulting in ineffective information security management and control, as well as an increased risk of security incidents.

(3) Employees with a low level of security awareness Employees are unaware of their own information security obligations at work, and many feel that information security is the responsibility of the IT department or system administrator. It is also unclear whether an enterprise's information security encompasses personnel data and storage media. According to statistics, internal employee information leakage,

whether deliberate or inadvertent, is the primary cause of information security concerns in most businesses. Employees' lack of security awareness is also a major source of hazard to company information security.

(4) Safety risk prevention and control capabilities are lacking. In reality, some businesses are unaware of the need of safety risk prevention and control in their operations and management processes, and they lack emergency reaction plans for "accidents and incidents." For critical information systems and materials, there is no backup strategy or recovery plan in place. An information security event may only be passively accepted or corrected once it occurred. Failure to achieve "prevention, control, and improvement afterwards" risk prevention and control management has had a significant impact on the continuity and reliability of business operations.

1.3 Information Security Management Systems

ISMS (Information Security Management System) is a novel concept in the field of information security that originated in the United Kingdom in 1998. As shown in Figure 1. In the sphere of information security, it is the application of Management System (MS) ideas and procedures. ISMS has been an effective technique for businesses of all sorts and sizes around the world to tackle information security concerns in recent years, thanks to the design and updating of ISMS international standards. ISMS certification has now become a useful tool for businesses to demonstrate their degree of information security and competency to society and its stakeholders. The meaning of isms is as follows:

- (1) A standard for building and maintaining an information security management system is the information security management system. According to the standard, businesses must build an information security management system by establishing the scope of the system, formulating information security policies, clarifying management duties, and selecting control objectives and control techniques based on risk assessment. system for managing information security;
- (2) The organization should operate in accordance with the system's requirements to maintain the system's effectiveness;
- (3) The information security management system should be documented, that is, the organization should establish and maintain a documented information security management system that describes the assets to be protected, the organization's risk management methods, control objectives, and so on.

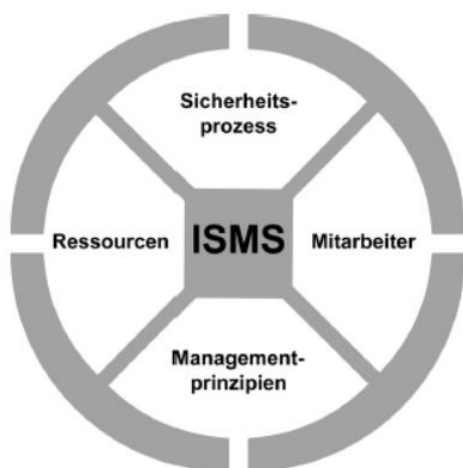


Figure 1. ISMS

2. Model Research

2.1 IS027001

Information security has become a priority for all sectors of society as the worldwide degree of informatization continues to improve. Particularly since the media has disclosed a succession of information security breaches in recent years, people from all walks of life have become more concerned about information security. The UK Department of Trade and Industry established the ISO27001 standard in 1993. The ISO27001 standard has been adopted by a wide number of nations and is the world's most representative information security management system. The ISO27001 information security management system standard can effectively secure information resources and facilitate the informatization process's orderly, healthy, and long-term development. When a company receives the ISO27001 certification, it signifies that the company's information security management is scientific and reasonable, and that it can effectively safeguard both customer and internal information. There can be numerous perks or advantages after completing the ISO27001 information security management system certification. Information management at all levels can be coordinated after the implementation of the information security management system, and management links can be simplified to increase management efficiency. Passing the ISO27001 information security management system certification can also help to improve the credibility of e-commerce transactions between businesses, establish a trustworthy cooperation connection between websites and trading partners, and advance company business informatization. Passing the ISO27001 information security management system certification will help organizations fulfill

their information security commitments, reduce customer and employee distrust, and increase corporate performance. The ISO 270001 model is shown in Figure 1.

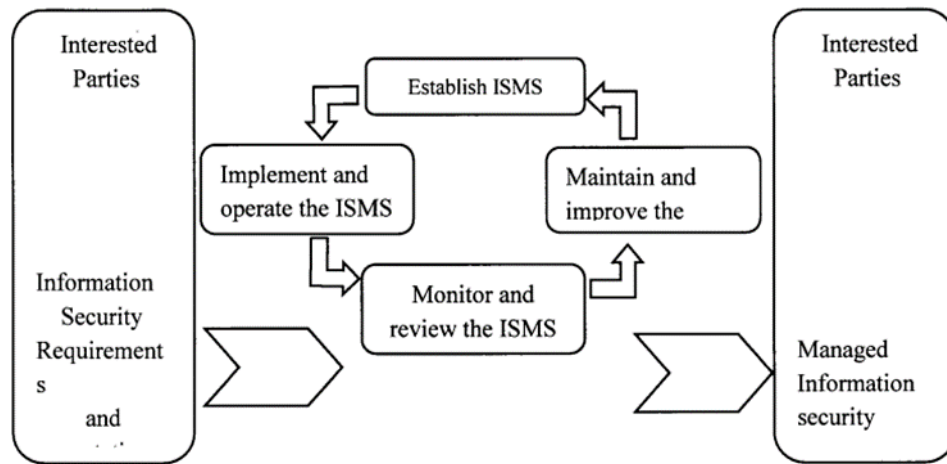


Figure 2. ISO270001 Model

2.2 COBIT

The Information Systems Audit and Control Association (ISACA) developed COBIT (Control Objectives for Information and Related Technology) as a complete framework for I&T governance and management. It can help management with IT governance and provide guidance. The company makes good use of information resources and manages information-related risks well. The standard system has been used in important organizations and enterprises in over 100 countries around the world, particularly since the introduction of the "Sarbanes-Oxley Act" in the United States and the relevant regulatory systems of my country's regulatory authorities, making internal control more strict and standardized. COBIT is a significant tool for developing IT internal controls that are compliant with these legal frameworks. ISACA has launched a set of COBIT 2019 framework products, which are open frameworks that can be customized.

There are currently four products available: COBIT 2019 Framework: Governance and Management Objectives, COBIT 2019 Framework: Introduction and Methodology, and COBIT 2019 Design Guidelines: Solution Design for Information and Technology Governance COBIT 2019 Guide to Implementation: Information and Technology Governance Solutions: Implementation and Optimization. COBIT is a governance and management framework for the IT components required by an enterprise to receive, process, store, and distribute information. It is not a framework for structuring business processes or for governing and managing all specific technologies. Figure 1 depicts the COBIT core model, which has five domains and forty governance and management objectives. Helping to achieve company goals is one of the most important aspects of delivering I&T value. These objectives are divided into five categories, each with its own set of governance and management objectives. Each of the 40 governance and management objectives is linked to a process, which is one of the governance components in this core model. COBIT 2019 defines applicable standards, guidelines, and compliance criteria for each governance component that can be referred to. Under each applicable component, it also contains thorough references and necessary guidance. COBIT is currently only employed by a few firms or government departments with a very high level of informatization due to the limitations of my country's informatization level. COBIT's five categories are concerned with organizing the whole life cycle of information system development and risk management. A comprehensive set of control methods and

technologies has been established. As a result, risks are recognized, assessed, and dealt with using the COBIT framework, and the design of system architecture and functions is carried out in a targeted manner, which is beneficial to the informatization of Chinese organizations, particularly the protection of sensitive data. The word "protection" has a lot of meaning.

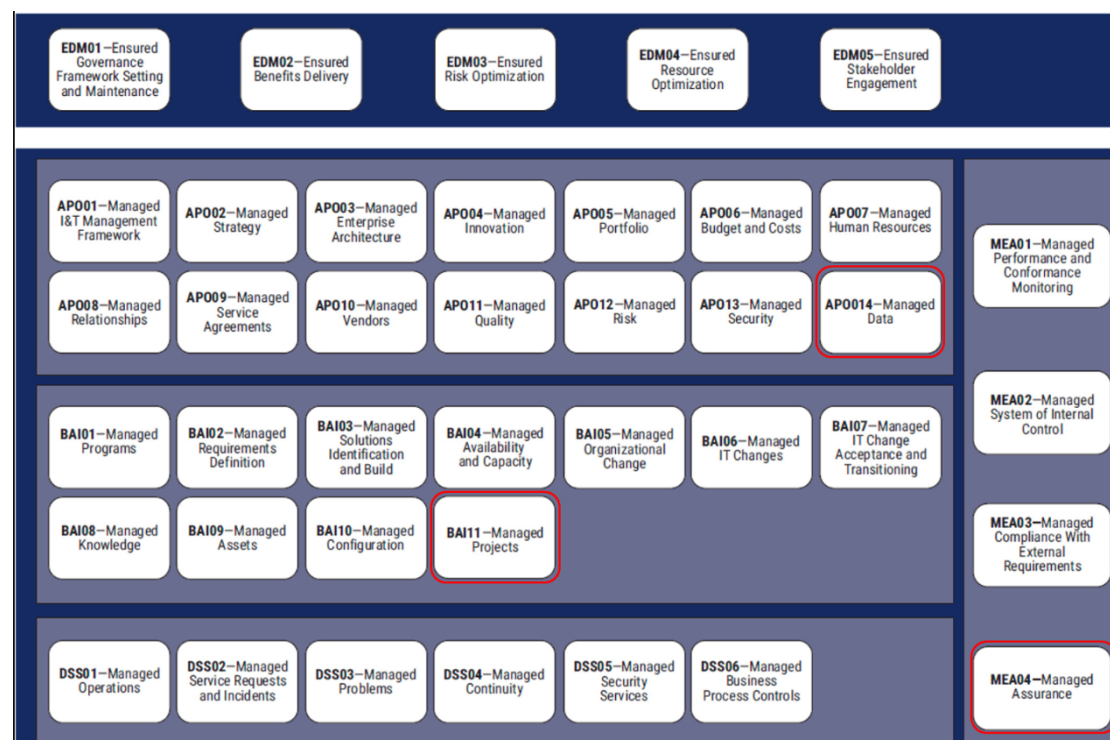


Figure 3. COBIT Framework: Governance and Management Objectives

2.3 ITIL

The Information Technology Infrastructure Library (ITIL) is a collection of best practices for IT service management. The UK government launched a programme in the mid-1980s to build a standardized and financially measured use of IT resources in order to improve the quality of IT services in government departments. ITILV 1.0 is the project's final product. The UK Department of Commerce (OGC) compiled best practices in IT service management from 2000

to 2003 and released ITILV2.0, which consists of six modules: service management, business management, IT service management implementation planning, application management, security management, and ICT infrastructure management. ITILV3 was officially released in 2007. It combines the greatest features of V1.0 and V2.0, incorporates current best practices in the field of IT service management, and for the first time introduces the idea of life cycle. IT services are continuously upgraded in a cycle using the PDCA paradigm (Plan-Do-Check-Act) to ensure ITIL's viability. ITILV3 organically combines numerous modules, uses service strategy as a guide, and continually improves the entire process through the execution of service design, service transformation, and service operation, thanks to the inclusion of the "life cycle model" in ITIL V3. The administration of IT services can be improved through continuous service improvement. Form a virtuous circle by integrating into a whole. ITIL is the world's most used management system for delivering IT services. In an emergency, broadcast instructions and verification code matching can be done, and satellite signals can be switched using an audio switching device. It will automatically switch to the standard tiny signal source after the transmission. GPS standard frequency generator equipment and digital FM synchronous exciter equipment can be used in the FM transmission system. It can effectively alter the signal and improve the overall work effect. Because emergency broadcasts are aired using the FM broadcast transmission system, the appropriate FM reception equipment must receive the emergency broadcasts in a systematic manner. The essential

emergency broadcast signals can be fully received in the vicinity via mobile terminals, handheld devices, and other devices to control the FM module. LED screens and multimedia control systems can also be used in heavily populated regions. Wireless receiver speakers are put in remote regions to help with broadcast-related emergency broadcasts.

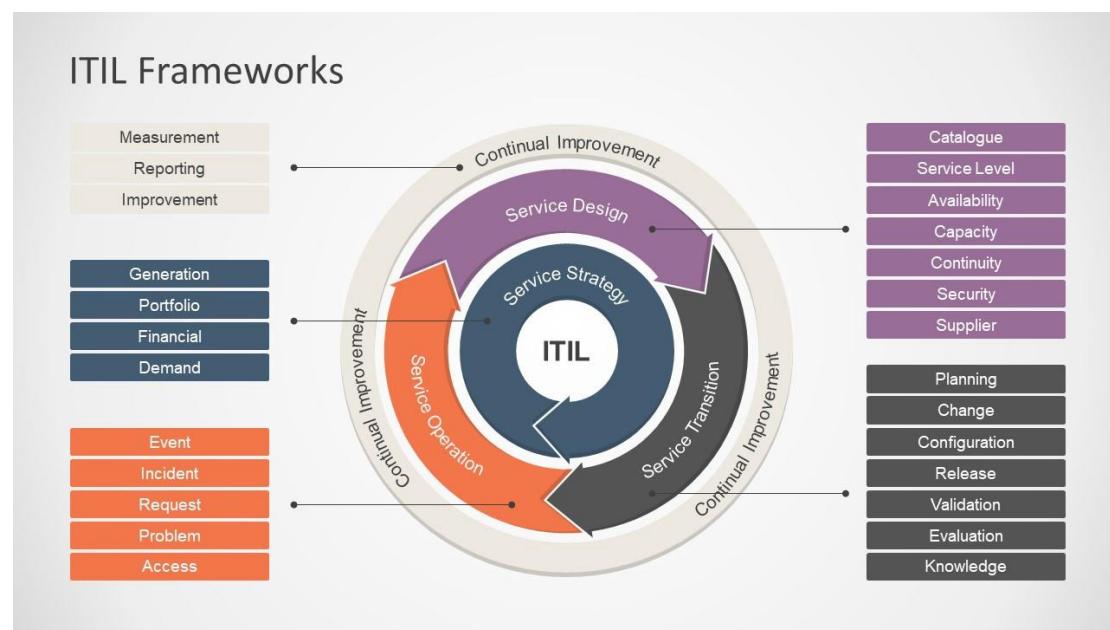


Figure 4. ITIL Frameworks[8]

2.4 DSMM (Data security capability maturity) model

DSMM—The Data Security Capability Maturity Model (DSMM) was developed in collaboration with more than 30 businesses and institutes by Alibaba and the China Electronics Standardization Study Institute, based on a lot of practice and research. The National Standards Committee published the "Information Security Technology Data Security Capability Maturity Model" (GB/T 37988-2019) on August 30, 2019. This standard can be used to assess an organization's data security maturity, as well as to assist industries, businesses, and organizations in

identifying data security gaps. It can also be used by competent authorities to manage data security. The type and scope of data will, in the end, improve data security and industry competitiveness across the board, ensuring the growth of the big data industry and digital economy.

The three dimensions of DSMM's architecture are as follows:

(1) Security capability dimension

The security capability dimension clarifies an organization's data security capabilities, encompassing organizational structure, institutional processes, technology tools, and personnel capabilities.

(2) Dimension of capability maturity

The maturity level of an organization's data security capability is classified into five levels: level 1 (informal execution), level 2 (planning and tracking), level 3 (complete definition), level 4 (quantitative control), and level 5 (full definition) (continuous optimization level)

(3) Process dimension of data security

The data security process consists of two parts: the data life cycle security process and the general security process. The data life cycle security process covers data collecting, data transmission, data storage, data processing, data exchange, and data destruction security.

3. Case study

3.1Case

Coffee Blue has locations around the world, and it typically uses cloud services to

supply information technology to its staff and customers. The corporation has recently been under a lot of pressure to utilise its employees and consumers because of its big staff base and multinational client base. Personal devices can connect to the company's network and resources. Companies are concerned about the protection of employee personal data and consumer data. The firm is also concerned about its extremely valuable intellectual property. They are looking for help from information security systems. This article's author tries to use ISO 270001 to deliver security information services.

3.2 Design Principles for Information Security Management Systems

- (1) The information security management system must be tailored to the company's needs.
- (2) The information security management system should include both security and efficiency.
- (3) The method for managing information security should be thorough.
- (4) The information security management system should be a dynamic system that may be improved on a regular basis.
- (5) The information security management system must balance technology and management equally.

3.3 System design and implementation

The objective of ISO 27001 is to maintain the application and increase the efficacy of information security management. The application of ISO 27001 is the process of information management, and its development technique is to control the

process. The ISO 27001 information security management standard is implemented by properly completing the PDCA cycle (standard ISO27001). Using the P-D-C-A method (Plan, Do, Check, and Act):

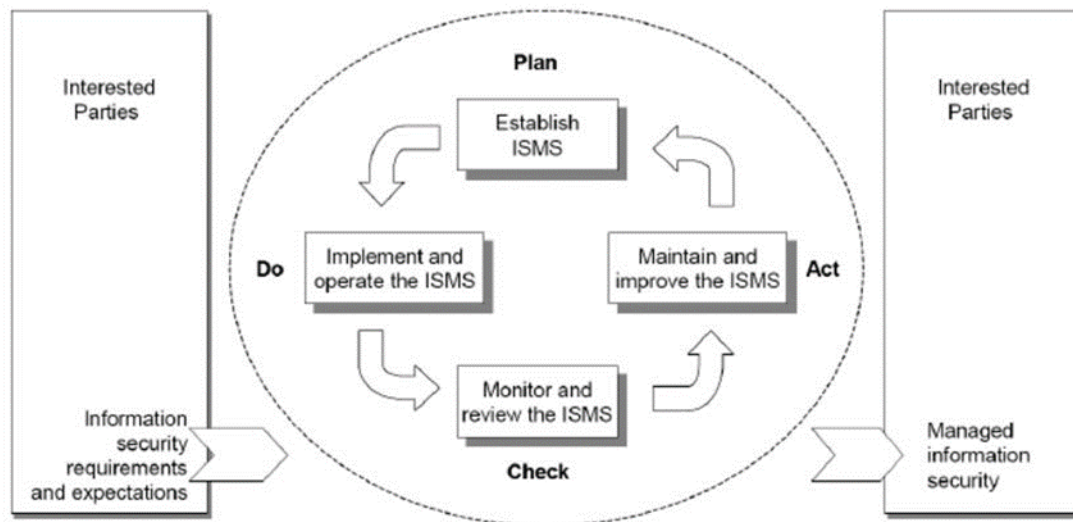


Figure 5. P-D-C-A Model

- (1) Preparation (creation of an ISMS): Establishing security policies, objectives, processes, and procedures linked to risk management and information security in accordance with the organization's overall strategy and objectives to produce outcomes for execution
- (2) (Implementation and Operation of ISMS): Security policies, controls, processes, and procedures are implemented and operated.
- (3) Inspection (monitoring and reviewing the ISMS): As needed, assessing and measuring process performance in accordance with the ISMS strategy, objectives, and prior experience, and reporting the findings to management for review.
- (4) Improvement (maintaining and improving the ISMS): Taking corrective and preventive actions in response to internal ISMS audits, management reviews, or other information in order to achieve continuous ISMS improvement. The P-D-

C-A model is a popular management process model. When the model is used, it is applied in the following order: P-D-C-A. In the management of an organization, a whole P-D-C-A cycle might be considered. The organization's management system will be improved to a certain extent after each P-D-C-A cycle, and the organization will enter the next higher management cycle at the same time. Through the continuous P-D-C-A cycle, the organization's management system will be continuously improved, and the management level will be continuously improved. Furthermore, ISO27001 emphasizes the importance of documenting the information security management process. Security policies, applicability statements (selected and unselected control objectives and control measures), program documents required to implement security controls, ISMS Management and operational procedures, and documentation of all activities undertaken by the organization around the ISMS should all be included in the ISMS document system.

3.4 The significance of the operation and maintenance system

In compliance with the ISO 27001 standard, the coffee shop has built a scientific and effective management system. It thoroughly evaluates and certifies its own network operation and maintenance management status and identifies any existing issues through analysis and certification. Standardize the creation of the actual network operation and maintenance service management system, guide its practice, and continuously enhance its own IT service management level by refining the internal process. The internal audit and management audit systems

have been clarified as a result of the building of the network operation and maintenance management system. Specify and guide the network operation and maintenance service management process by writing documentation and sorting out the network operation and maintenance service management process. Event management is realized, and operation and maintenance data is accumulated, which is used to improve the input of the process, the process specification is clear, the service level is improved, and the business relationship is good, thanks to professional operation and maintenance management software tools. The PDCA approach is used to continuously optimize and improve network operation and maintenance services in order to achieve ISO 27001 standard implementation and gradually improve network operation and maintenance service management.

4. Conclusion

The role of information security is becoming increasingly vital as science and technology grow, as well as the rise of informatization. The dual pressures of information technology development and information security are exerting themselves on businesses. They must urgently improve information system security management, embrace common industry standards, and establish an information security management system that satisfies their particular development requirements.

Based on the project's actual experience and research into the information security management system and risk management, this paper proposes a PDCA

closed-loop enterprise big data security architecture framework model based on the enterprise's information security characteristics, which ensures the project's orderly development and smoothness. implement.

Reference

- [1] Liang Duan, Zhou Yingyao. Research on PDCA closed-loop enterprise big data security architecture framework model [J]. Electrical Technology, 2020(11):133-135.
- [2] Liu Xia. Planning of Information Security Management System Based on ISO27001 [J]. Computer Knowledge and Technology, 2010,6(10):2337-2339.
- [3] Liu Xia. Planning of Information Security Management System Based on ISO27001 [J]. Computer Knowledge and Technology, 2010,6(10):2337-2339.
- [4] Zhou Min, Chen Zhihua. Research and Design of ITIL-based Operation and Maintenance Service Management System [J]. Information Security and Technology, 2012,3(5):8-10,16.
- [5] Wang Yang. Design and Implementation of Risk Assessment System Based on ISO27001 [D]. Liaoning: Dalian University of Technology, 2007.
- [6] Liu Chunqiang. The application of ISO 27001 standard in information security management of Alstom [D]. Beijing: Beijing University of Chemical Technology, 2015.
- [7] Meng Fanfei. Research on IT Governance and Risk Management Based on COBIT Framework [J]. Shanghai Business, 2021(1):30-32.
- [8] MunnaPrawin. Overview of ITIL