

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

Name: Xu Zhang

Student number: 2200467

Major: Software Engineering and Artificial Intelligence programme

Email: 2200467@student.uwtsd.ac.uk

Abstract- Under the development trend of digital economy, information security, data security, data sharing and openness are getting more and more attention. The explosive growth of data and information and the massive collection of data and information hold great value. But at the same time, the leakage and misuse of data and information occur from time to time, this situation can cause huge losses of interests to individuals, enterprises and even the country, so the issue of data information security has become a major issue related to national security and economic development, and the vital interests of the general public. CoffeeBlend company as one of the world's best blended coffee company, IT services and online business, etc. Internet applications are indispensable in the company's operation. In this paper, we go through the cybersecurity issues of CoffeeBlend Company and design a rational approach to maintain the information security and compliance of the company based on various security frameworks and aspects such as Information Technology Infrastructure Library (ITIL), ISO2000, etc. Finally, the impact of new regulations and standards on information security is critically analyzed.

Keywords: data and information security, ITIL, ISO2000

I. Introduction

With the booming development of Internet information technology, more and more enterprises are providing various services to Internet users through websites or applications. While enjoying various dividends brought by information technology, enterprises are also facing threats and challenges from information security. With the diversification of Internet viruses, the organization of hacking behavior and the increasing reliance of enterprises on the Internet, information security has become a prominent issue. If a serious information security incident occurs in an enterprise, it will have serious impact on its assets, reputation and even continuous operation. Therefore, it is necessary to make information security an important part of the company's development strategy, which is significant for the company's development.

In recent years, the frequent occurrence of enterprise network security incidents, including common DDoS denial-of-service attacks, remote command execution, sensitive information leakage, webpage tampering, Trojan horse viruses, etc. like the "Wanna Cry ransomware virus" that affected the world in 2017, causing more than 100,000 hosts around the world to be infected and massive data data permanently lost, bringing unpredictable losses 错误!未找到引用源。 In response to the above severe network environment, people are making progress in information security management standards and have designed information security management standards to meet their own

needs [2]. And as the concept of information system security continues to develop and improve, information security has gradually evolved from early communication security to information security assurance. 1998, the U.S. National Security Agency released the most representative Information Assurance Technical Framework (IATF) in the industry, which has played a good role in guiding the construction and development of various information security assurance systems. The International Organization for Standardization issued ISO/IEC 27001:2013 in October 2013, which is a common standard for information security management system generally recognized by all countries in the world at present [3].

In terms of factors influencing information security management, Hemth T (2009) studied the impact of employee behavior on enterprise information security management, and the results showed that information security training and education and a clear penalty mechanism would make employees more compliant with information security policies, proving that the environment can have an impact on different security behaviors of people [4]. Muktesh Chander (2013) found in his research that the system and norms of information security management, the shape of information security organizational structure, the level of leadership involvement, and information security awareness training and education all have an impact on information security management [5]. Aleksandr Ključnikov (2019) suggests that the four main factors of information security management are the consistency of information security management with the business activities of the company, the support of top management, the security culture of the organization and the degree of implementation of security management measures [6]. Kobis Pawel (2021) indicates that the impact of human factors on information security management cannot be ignored either [7].

Last but not least, as a qualified IT staff, you need to do the following in order to better maintain the network environment.

1. Remember the network basics, including the network topology, basic network configuration methods, etc.
2. Improve basic personal skills, such as language skills, hard-working spirit, group work ability, etc.
3. clarify the scope of job responsibilities and basic processes, and distinguish the difference between the work content of Internet work and enterprise area network work. And familiar the workflow with the network set-up, hardware and software upgrade, network fault detection.
4. Need to have perfect personal basic skills, in terms of hardware, with the ability to plan the whole network environment and the ability to maintain network equipment. In terms of software, master the general installation and

configuration methods of network operating systems, as well as the skilled configuration and use of application software.

II. Related methods

A. ISO27000

A key aspect of the development of information security management is the move toward an era of systematic and standardized management. The ISO27000 family of standards is the collective name for a set of specifications set aside by the International Organization for Standardization for information security management systems, and the ISO27001 specification is a set of standards for establishing information security management systems, with the full name "Information technology - Security techniques - Information security management - Requirements" [8], which provides a detailed description of the requirements for how an enterprise can build, implement, maintain, and improve an information security management system. ISO27001, as a set of management specifications, guides the relevant managers to apply the information security management system, for example, with the goal of building an information security management system that meets the actual needs of the company.

The ISO27000 family of standards contains a total of 29 standards, and most of the standard specifications have become recognized and accepted as general safety standards by many organizations [9]. The most important of these members and their main contents are shown in Table I.

Table I. ISO27000 members and main contents

Name of standard	Main contents
ISO/IEC 27000	Information security management system basics and terminology
ISO/IEC 27001	Information security management standard requirements
ISO/IEC 27002	Information security management practice guidelines
ISO/IEC 27003	Information security management standards guide
ISO/IEC 27004	Information security management monitoring and measurement
ISO/IEC 27005	Information security risk management

Information security management controls are typically constructed in fourteen areas to establish best practices for information security management, guided by the controls of ISO 27001 [8]. The fourteen areas are: information security policy, information security organization, personnel information security, information asset management, access control, cryptography, physical and environmental security, operational security, communication security, system development management, vendor relations, security incident management, business continuity, and compliance.

Information security standards are the essence of practical experience of excellent enterprises, and can be used as the theoretical basis for information security management of enterprises. Therefore, based on the full understanding of these information security management theories and standards, and then combined with the actual situation of the enterprise, this is an important guidance for the research of information security management issues and the design work of the optimization plan of company.

B. PDCA Cycle Model

The PDCA cycle is a common process model in management often used for continuous improvement of product quality [10]. The PDCA management model for continuous improvement is divided into four phases: P-Plan, D-Do, C-Check, and A-Activation. It divides the task into

steps such as developing the plan, implementing the plan, and checking the effectiveness of the implementation. And at the end, the successful part is incorporated into the specification and the part to be improved is placed in the next iteration cycle to be addressed. The PDCA management model is shown in Fig. 1.

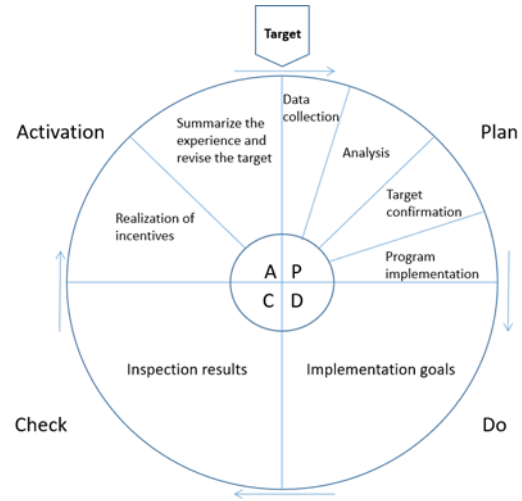


Fig. 1 PDCA management model

The ISO27001 standard is based on the theory of PDCA to establish and optimize the information security management system. And after the cycle of P-D-C-A iteration, the enterprise can transform the specific information security objectives and requirements into a manageable and controllable information security management system.

C. Secure Development Life Theory

Secure development lifecycle (SDL) is a management model that guides and regulates the software development process from a security perspective, helping developers to create more secure and reliable software products and reduce production costs while meeting security requirements [11]. The purpose of security development is to integrate security into every phase of software development. Secure software systems are built by adding appropriate security activities in the phases of requirements analysis, system design, functional verification, system release and maintenance. Fig. 2 shows a sketch of the SDL security activities proposed by Microsoft.



Fig. 2 SDL Security Activities

The core concept of SDL is to integrate security considerations into all phases of software development, and enterprises can effectively improve the security of their business systems by building a secure development lifecycle management mechanism that suits them.

C. ITIL

The Information Technology Infrastructure Library (ITIL) was developed in the 1980s by the CCTA, a UK government department, and then transferred to the OGC, the UK Department of Commerce, to manage and use for IT services [12]. Many famous companies such as IBM, HP, Microsoft, etc. have developed perfect IT service management platform software based on ITIL management theory, which is widely used in various industries to improve service quality, enhance management level, and increase

enterprise production efficiency. In short, ITIL theory can be well infiltrated into enterprise applications and practices, and the theory can also keep pace with the development of information technology, and constantly iterate and update.

The difference between traditional IT management systems, which are technology-centric, and the ITIL theoretical framework is that its management system is process-based and ultimately serves the customer. Through the appeal transformation, it can complete the transformation from the traditional management approach to a service-centered approach. The basic framework of ITIL is shown in Fig. 3.

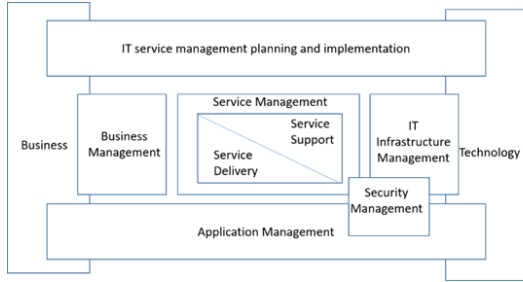


Fig. 3 ITIL foundation framework

The main ITIL framework diagram shows the business management, IT infrastructure management, Application management, IT service management planning and implementation, security management, and service management modules and the relationship between each module and the business and technology. The Service Management module is at the core of the framework, and the other modules rely on Service Management to communicate with each other and together form the main ITIL framework. Service Management can be divided into two groups: service support and service delivery, which manage IT service content and IT service processes respectively.

For the introduction of core modules, the service provisioning group in Service Management mainly manages the provisioning content of IT services, including service level management, service capability management, availability management, IT service-related financial management, and continuity management. The service support group in Service Management mainly manages the organizational process of IT service acquisition by users, including service desk functions and several core processes such as events, changes, problems, configuration and release.

III. Example Application

A. CoffeeBlend Introduction

CoffeeBlend, as a large Internet-dependent company, data and information is one of the core assets of the company. And the company may have problems such as intrusion of cloud service platform, wireless network failure, employee and customer information theft, intellectual property leakage, etc. The occurrence of information security issues can bring extremely high security risks and loss of economic benefits to the company. Since the actual situation of each enterprise is different and the information security needs are also different, the actual situation of information security management of each enterprise is different and lacks universality. For this reason, it is necessary to conduct a suitable information security analysis for the current information security

management status of CoffeeBlend. Based on various methods of protecting information, we propose appropriate solutions to reduce the harm caused by information security risks to business operations.

B. Information Security Policy

For the information security problems of CoffeeBlend, an information security management system prototype can be built based on the above theoretical knowledge and the experience of other similar-sized enterprises. The information security management system is built from four modules, including security policy, laws and regulations, organization management, and technical protection, to meet the needs. The four modules contain a total of 15 areas such as Legal Regulations, Organizations, Data Security, etc. The information security management system is shown in Fig. 4.

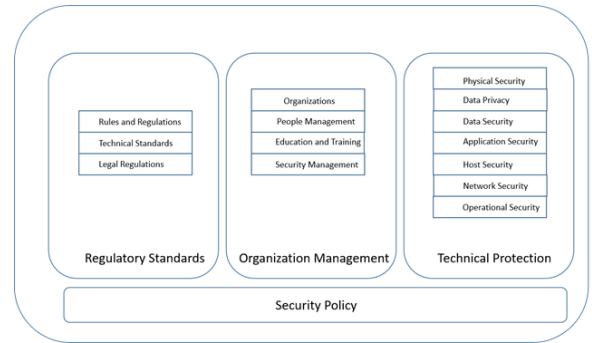


Fig. 4 Information security management system

Comparing with the definition of control objectives and measures in ISO27001 information security management standard, there is a certain mapping relationship between CoffeeBlend's information security management system and the definition of ISO27001 standard, such as CoffeeBlend's "regulations", "technical standards" and "security policy" correspond to "information security policy" in ISO27001.

In addition, the information security organization structure set up for it is as follows in Fig. 5.



Fig. 5 Information Security Organization Structure

The information security organizational structure of the company is divided into decision-making level, management level and executive level. The decision-making level is the information security management committee, which is mainly responsible for the company's information security strategy decision and the formulation of security policy objectives. The management layer is composed of a combination of heads of various security departments. The executive level divides information security into different departments for management according to specific responsibilities, and each department includes many teams such as data center platform security team, business security team, office information security team and content security team.

In the face of various possible scenarios, the above information security management methods may still have some problems:

1. The information security policy is not effectively implemented, and the company's information security system is not communicated and implemented by all employees after it is formulated, and the employees are not informed of the information security related system through effective channels, resulting in the problem that the information security policy is not effectively implemented.

2. The awareness of information security of personnel is weak, and many personnel cannot record security events in time. And it is always easy to ignore the danger of virus emails and easily click on harmful links, which leads to the loss of company information.

3. Information asset management is not standardized, and the company lacks a unified and standardized information asset hierarchy management standard. Many core technical documents are not stored in secure computers, and once any employee's office computer is hacked, a series of core technical documents may be illegally accessed.

4. Failure to identify security risks in system development and management leads to frequent system vulnerabilities. Most of these vulnerabilities have been introduced in the development and construction of the system, and the development team, due to the lack of security expertise and experience, cannot foresee potential security risks at the early stage of the development and construction of the system, thus jeopardizing information security.

C. Information Security Policy Optimization

In this paper, we propose the following optimization scheme based on the principles of compliance, wholeness and practicality to address the above possible problems.

1. Information security policy optimization

Information security policy is the cornerstone of the information security system of the whole information security project, and is an important foundation of the information security management system. According to the problems in CoffeeBlend's information security policy, the following aspects are optimized to achieve the company's security goals

(1) The construction of information security document system architecture and the establishment of a perfect information security management system are the key guarantee for the realization of the company's information security objectives and the important guarantee for the orderly and efficient promotion of information security work. Referring to ISO 27001 security management system standard, we design the document structure of information security management system of the company, and divide the document system into four levels of pyramidal structure. In the order from top to bottom, the top-level document is the information security policy manual, which serves as the overall platform of BC's information security management and guides the construction of the enterprise internal security management system. The second level document is a further refinement of the overall policy, defining the main system strategies and control points of each control area of information security management. The third level document is the security system specification and technical standard. The fourth layer of documents is the specific operation procedures, checklists, guidelines and implementation details and other operation guidance manuals, which are used as guiding manuals for

security implementation personnel. The architecture is shown in Fig. 6.

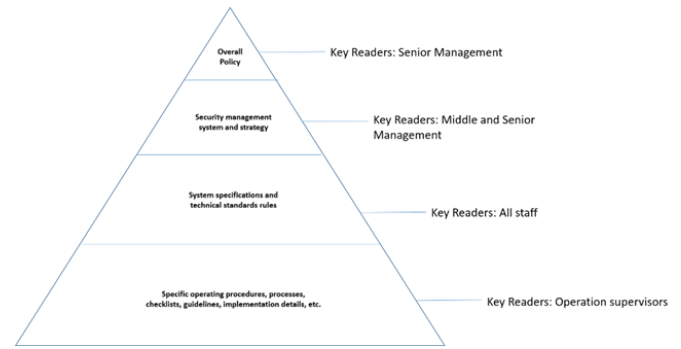


Fig. 6 Information security management document system

(2) Establish a system for continuous improvement, and establish a system for information security management for Company CoffeeBlend that can be continuously improved using the PDCA cycle model as a guiding theory. P indicates the plan for information security management policy, D indicates the implementation of an information security management policy, C indicates the supervision and review of information security management policy and its basic process is shown in the Fig. 7, A indicates the maintenance and improvement of the information security management policy.



Fig. 7 Basic process of supervision and review

2. Personnel information security awareness enhancement

For information security control measures to be implemented smoothly, all company personnel should be deeply aware of the importance of information security, enhance their own information security awareness, and learn and comply with the company's information security system and protocols. The following aspects are used to enhance the information security of personnel.

(1) Information security control before and after the employment of personnel. Before employees join the company, they need to be reviewed for information security. After joining, sign the necessary contracts and information security confidentiality agreements with them to clarify confidentiality obligations and responsibilities. At work, the implementation of information security work is included in the results of employee stage assessment.

(2) Vigorously promote the concept of corporate information security to employees so that they are aware of the importance of information security. Conduct regular security education and training to let employees understand what information security is and how to maintain it.

3. Information asset management optimization

Information assets are information resources that are held or managed by an enterprise and can bring benefits to the company's future operation. To implement effective protection of enterprise information assets, we must first determine which information assets the company currently owns, list the asset catalog, understand which information assets need to be protected. And then implement appropriate hierarchical protection according to the importance and risk level of information assets, and reasonably define the

attribution and protection responsibilities of information assets.

(1) Information asset classification management, information asset classification management is indispensable in the process of information security management. And the classification of information assets is the basis of reasonable allocation of operation and maintenance personnel's energy in the process of system management. According to the recommendation of ISO27001 information security management specification, data assets can be defined as follows: secret data, confidential data, internal data, and public data.

(2) After the reasonable classification and grading of information assets, it is also necessary to sort out the management process of assets, define the attribution and management responsibilities of information assets, operation processes and specifications, etc. For online business services, it is required to do disaster recovery and backup of assets, multi-point access and other measures to improve the disaster recovery capacity of business and ensure the expected availability of service assets. In addition to that, corresponding security administrators should be assigned, and the security administrators should regularly conduct security risk assessment, control access list checking, ensure the security of data and equipment, and other duties to ensure the security of data assets.

4. Improvement of system development management

To solve the problem of frequent system security vulnerabilities at CoffeeBlend, it is necessary to intervene in security activities early in the system development cycle. The security development lifecycle theory can be used to guide the design of a security improvement plan for system development management.

(1) Security development lifecycle management is to intervene security activities in all phases of business system development. For the actual situation of relatively weak security foundation of the company's team members, in order to ensure that they understand the relevant security-related basic knowledge, need to be established at the beginning of the project by the security team to conduct appropriate security training for business system developers. At the same time, the security requirements need to be clarified with the team, focusing on four basic elements: security acceptance criteria, security intervention time, security self-test products, and recommended implementation roles.

(2) In order to effectively identify security risks in the development phase, security requirements need to be implemented in the system design phase around several aspects such as security design requirements, attack surface inspection and threat modeling. And the security personnel will guide the system-related responsible persons to conduct self-inspection and output security inspection report, so as to promote the implementation of security rectification items.

The above optimization plan is an improvement for CoffeeBlend's information security management. Finally, for the question of why new standards and regulations appear constantly, my understanding is this: the times are not unchanging, in the face of the rapidly developing Internet era, new technologies are emerging, the way of harming

information security is also changing, and people's demand for information is getting bigger and bigger. In order to cope with this situation, we also need to constantly develop new information security standards and regulations in order to keep pace with the times and adapt to such changes so as to achieve the purpose of maintaining good information security in all aspects.

IV. Conclusion

This paper examines the importance of information data security in today's Internet era and analyzes the development and construction of information security management with reference to relevant literature. In the face of various cyber security issues that infringe on information security, using the information security issues that exist in CoffeeBlend as an example, this essay explores the theoretical knowledge of information security such as various security models, Information Technology Infrastructure Library (ITIL) and ISO 27000. It also uses this as the basis for proposing the information security management system and the security organization structure of the company. For some possible shortcomings in the solution, corresponding optimization solutions are also proposed in terms of information security strategy, personnel information security awareness, etc. Finally, the emergence of new standards and regulations is critically analyzed, and only through continuous improvement of standards and regulations can we keep pace with the Internet era.

REFERENCES

- [1] Mohurle S, Patil M. A brief study of wannacry threat: Ransomware attack 2017[J]. *International Journal of Advanced Research in Computer Science*, 2017, 8(5): 1938-1940.
- [2] Liu S. Research on Core Technology Based on Computer Information System Security Architecture[C]//2018 3rd International Conference on Mechanical, Control and Computer Engineering (ICMCCE). IEEE, 2018: 607-610.
- [3] Humphreys E. Implementing the ISO/IEC 27001: 2013 ISMS Standard[M]. Artech House, 2016.
- [4] Herath T, Rao H R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness[J]. *Decision Support Systems*, 2009, 47(2): 154-165.
- [5] Chander M, Jain S K, Shankar R. Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach[J]. *Journal of Modelling in Management*, 2013.
- [6] Ključnikov A, Mura L, Sklenár D. Information security management in SMEs: factors of success[J]. *Entrepreneurship and Sustainability Issues*, 2019, 6(4): 2081.
- [7] Kobis P. Human factor aspects in information security management in the traditional IT and cloud computing models[J]. *Operations Research and Decisions*, 2021, 31.
- [8] International Organization for Standardization. ISO/IEC27001-2013. Information technology-Security techniques-Information security management systems-Requirements[S].2013.

- [9] Prislan K, Bernik I. Risk management with ISO 27000 standards in information security[J]. Inf. Secur, 2010: 58-63.
- [10] Omens D R. PDCA at the Management Level[J]. Quality Progress, 2006, 39(4): 104.
- [11] Gonchar L. Implementation of Secure Software Development Lifecycle in a Large Software Development Organization[C]//21st International Workshop on Computer Science and Information Technologies (CSIT 2019). Atlantis Press, 2019: 137-139.
- [12] Dabade T D. Information technology infrastructure library (ITIL)[C]//Proceedings of the 4th National Conference. 2012: 25-26.