

Research on Data Security, Governance and Compliance of Company CoffeeBlend

Abstract

Companies nowadays are becoming more and more reliant on information technology, which has led to various issues with information security. Following a review and study of pertinent papers, this article explains and contrasts the PDCA cycle technique, the ISO27001 standard, and the PAS99 specification in order to comprehend the distinctive features of each standard and the business risk management procedure. Separate presentations were made of the traits of these standards and the corporate risk management procedure. The ISO27001 standard is then used in this piece to assist the CoffeeBlend firm in developing its information security mechanism based on its security circumstances. As a consequence, a system for managing information security has been built that satisfies both the company's commercial goals and the requirements of global standards.

1 Introduction

In the process of the rapid development of network services, the internal management of Internet companies is also facing major challenges. the forms of service products are more and more diversified, and the boundaries of information security are different. the company's management of information security extends from the traditional network layer to the application layer. These changes increase the comprehensive demand of the company in terms of the subdivision and integration of service resources, the control of service process, and the ability to identify and deal with security risks. Information security is not only a technical issue, but also a consciousness and management issue. The company needs to sort out and improve the ability of security management by improving security management measures, taking the information security management model as the guidance, the security management of information resources as the goal, and the risk control as the process. Build an information security system that meets the requirements of the company and policy, help the company solve security problems, and help the company develop rapidly.

2 Survey of security frameworks

2.1 PDCA cycle method

Information security management system is the best practice of information security in the world, mainly through the IP0 process. Build the ISMS system within the enterprise, and realize the enterprise information security through the continuous improvement of PDCA. As shown in figure 2-1, the process implementation method is as follows:

Plan: according to the organization's information security requirements and other compliance requirements, define the scope and strategy of information security, and

establish the objectives, strategies and strategies of the corresponding risks of information security by evaluating the risks of information security.

Do: the process of implementation, in accordance with the selected control objectives, strategies, and policies.

Check: check the implementation of the plan and verify the implementation effect by means of monitoring, audit, review, evaluation and other means according to objectives, legal and regulatory requirements, strategies and strategies.

According to the inspection results, Action is effective for policy suitability and information security management system.

Conduct sexual evaluation, standardize and popularize the successful experience, and make continuous improvement in the problem part.

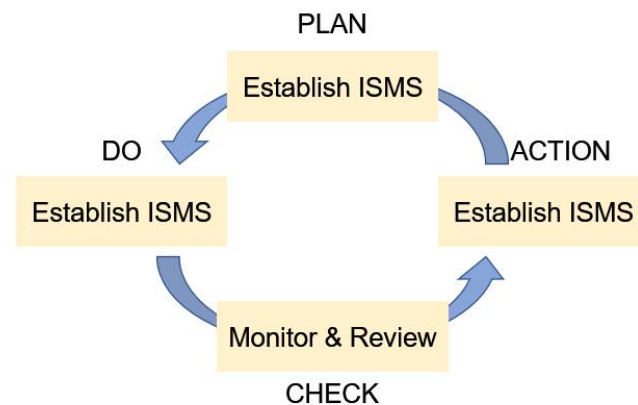


Figure 2-1. PDCA cycle

2.2 ISO27000 series requirements of information security management system

ISO/IEC 27000 is the general name of a series of related standards specially established by the International Organization for Standardization for the information security management system. Through the ISO27000 standard, we can build a set of non-constant and perfect information security management system for enterprises, including strategy, policy, policy, system, process, guide and recording. At the same time, combined with the PDCA process method, we can finally implement the information security management system and improve the level of information security management. The ISO27000 series focuses on the process, methods, and effectiveness of information security management. The internationally recognized standards include the requirements of the information security management system of "ISO/IEC 27001 2005" and the implementation guide of information security management of "US0/IEC 27002VR 2005" and so on.

2.3 PAS99 specification

PAS (Publicly Available Specification) is compiled by BSI (British Standards Institute) for those who established and implemented ISO9001. Integrated specifications by several standard organizations, such as ISO 14001, ISO/IEC 2700K ISO/IEC 20000, and OHSAS 18001.

At present, most of the organizations that have established management systems adopt or are using two or more standards and norms, and most of these management

systems operate independently. Through the research, it is found that there are some common elements in these management systems that can be managed in an integrated way, that is, to identify and optimize the basic consistent elements in multiple management systems. The PAS 99 specification defines general management system requirements. Although PAS 99 can not break away from the original standard requirements, it can build multiple management systems into a unified management system.

3 Main Problems in current CoffeeBlend Data Security Management

3.1 Lack of data security strategy and institutional system support

Entering the Internet era, the security capability of data services is related to the survival and development of companies. In the complex and changeable market competition, data security accidents may bring a fatal blow to companies. From the perspective of data security management, the establishment of an effective data security organization and the formulation of clear data security objectives and policies have become the core and necessary conditions to ensure the successful implementation of data security management within the company. companies must have the strategic consciousness of data security and plan the data security guarantee system from the top of the company, so as to reduce the risk of security operation to the greatest extent and protect the self-interests of the company.

CoffeeBlend has not issued the overall security strategic policy, security policy and institutional system of the company, and there is no unified understanding of the data security management framework and norms within the company. More importantly, the company uses cloud services to provide IT services to its employees and customers. In the face of the more complex security risks of cloud computing, the lack of security awareness and the lack of security strategy and policy system have rapidly increased its operational risks.

CoffeeBlend needs to establish overall data security objectives and policies, security strategies, improve the system as soon as possible, implement the data security leadership responsibility system, establish the awareness of all staff to participate in data security work, and reasonably control data risks through the integration of efficient data management system.

3.2 Data security technology capability needs to be strengthened

CoffeeBlend faces the lack of technical requirements and problems in cloud services. In summary, there are important risks and hidden dangers in the following aspects.

1) there are loopholes in security boundary protection, and there is a risk of data disclosure in illegal outreach.

2) user authentication is lack of two-factor protection, and there is a risk of user identity being used falsely.

3) intellectual property rights, company data and user data are not separated and prioritized, so there is a great risk of data theft.

3) the risk of security audit is high, and the audit scope is incomplete in both

network communication and data security, and the risk is high.

4) allowing their employees and customers to use their personal devices to access the company's network / resources is an important risk of data leakage for cloud computing services and must be taken seriously.

5) lack of anti-virus and anti-malicious code capabilities. Virus and malicious code intrusion is one of the most important security risks for CVM users, and effective protection capabilities must be provided.

6) there is a lack of technical ability and awareness in data backup and storage disaster preparedness, and there is a security risk that data damage cannot be recovered.

Therefore, in today's increasingly rich network cloud computing service model, CoffeeBlend urgently needs to carry out carding and inspection at the technical management level, through continuous learning and improvement, in order to fully meet the data security management needs of the future business.

3.3 The operation and maintenance system and measures of data security are not perfect

Cloud business makes extensive use of network virtualization, storage virtualization and computing virtual energy technology, and the deployment of assets and management rights is more reflected in logical identification.

CoffeeBlend lacks the list and classified management of data security assets, so for data security management, it is impossible to define the scope boundary of data assets at first, so it is impossible to implement management and control work effectively.

CoffeeBlend does not set up a security management center to centrally manage trusted communications, which can no longer meet the real-time authentication and audit requirements of cloud computing services throughout the business process, and there is a risk of identity fraud and data disclosure.

Business data security and backup strategy management are missing. In the previous traditional business of CoffeeBlend, most of the user business data are regulated as user self-management, and a few entrust value-added services for users, which are managed according to service items.

Therefore, it completely ignores the importance of business data security management and backup management, and there is no clear requirement of data security management.

With the development of cloud business, users' business data is deployed on the cloud platform, which has a great responsibility.

In the event of a system crash and data corruption, the loss is incalculable if it cannot be recovered.

CoffeeBlend does not formulate emergency procedures and emergency plans for various systems related to IT operation and peacekeeping data security according to traditional business, and there are still many problems in the update and release, training and drills of the plans.

There are many deficiencies in emergency plans for cloud computing, business

software, data protection and so on. at the same time, there is a lack of targeted training and drills for each plan, so it is difficult to predict the recovery cycle and effect after major failure.

Therefore, combing and improving the operation and maintenance management measures according to the standards of the data security management system and improving the guarantee capability is an important means for CoffeeBlend to alleviate the risk pressure of cloud service data security in the future.

4 Optimization Scheme of CoffeeBlend Data Security Management

4.1 Constructing the improvement Scheme of data Security Policy

Company data security policy is the goal and principle for companies to implement security management, which includes three aspects: companies formulate security policies and strategies according to their own security needs; companies improve safety management documents according to national policies and industry standards; companies form a top-down security management system including security strategy, management system, operation process and management records according to the needs of internal security management.

In the current mainstream information security management system norms, whether hierarchical protection or ISO27001, it is clearly pointed out that the primary task of building an information security management system is that the organization needs to establish a unified information security management policy and security strategy to ensure the implementation of security management, in other words, it is necessary to have a comprehensive information security awareness and core ideas from the high level of the organization.

According to the investigation of CoffeeBlend, it can be found that the company is currently lack of security strategy at the level of information security management, resulting in unclear security thinking and unclear working methods.

Therefore, we first formulate the security policy and security policy of CoffeeBlend, as shown in Table 2-1.

Name	Content
Aim	Implement risk control, pay equal attention to technology and management, improve safety and supervision, and make continuous improvement. Ensure the security, stability and continuity of the operation of the information system, ensure the availability, integrity and confidentiality of information data, prevent the information system from being attacked and destroyed, and prevent data leakage.
Range	All personnel of the company, business information assets, third-party security service providers, media.
Overall safety policy	Under the guidance of the idea of hierarchical protection, establish and improve the policy strategy and system system of information security management, improve the level of technical security, implement the system construction and operation and maintenance system, and establish a comprehensive security framework.
Principle	Leadership responsibility system, full participation system, authorized examination and approval system, continuous improvement system, policy coordination and regulation.

Table 2-1 CoffeeBlend Data Security Policies and Strategies

4.2 Improve the improvement plan of security organization

In the work of information security management, companies should improve the organizational framework of information security management as soon as possible, and the security management group should be responsible for the formulation and release of company security policies, security technology policies and standards as a whole. Supervise and guide the operation of information security activities in accordance with the company security policy framework. The security organization of an company should include leadership, management and implementation, with clear responsibilities and powers to supervise each other.

The main problem of CoffeeBlend is that the information security management organization and responsibility department are not clearly set up, which results in the fact that the information security posts and responsibilities are not clear, and the responsibility of security management is very vague. Therefore, on the basis of the construction of information security management policies, CoffeeBlend needs to implement the following two improvement measures.

1) Establish the organizational framework for the implementation of information security in CoffeeBlend, set up a responsible information security management working group led by the head of the company, and implement the overall plan planning and management of information security in the company as a connecting link. The members of the information security management team must include a vice general manager of the company, managers of various business departments, information security personnel and manpower specialists, and the company leader shall act as the group leader. The department in charge of information security shall be set up within the company to be specifically responsible for the implementation of

security management, set up subdivided information security management posts, and clarify job responsibilities and qualifications. Standardize the authorization and approval process and audit process of various business operations. Hire a third-party security expert as a security consultant to guide company safety management.

2) Guard against customer access security: in companies, managers tend to pay more attention to daily workflows and controls, but it is easy to ignore the control of external access. because CoffeeBlend allows its employees and customers to use their personal devices to access the company's network / resources, coupled with customer behavior uncertainty and information differences, it is necessary to pay more attention to the effective control of such access in the field of information security.

4.3 Improve the management system of safety operation and maintenance

By setting up an efficient security management area, the unified management of systems, products, equipment, information security events, operation flow and strategic configuration can be realized. CoffeeBlend needs to establish a cloud service security management center, in which the security management area establishes a security management relationship with other business areas through private IP addresses, and sets security control policies on the boundary of the zone through a firewall to ensure the security isolation of the security management area. Through the cloud service security management center, CoffeeBlend can centrally implement unified management, configuration and security policy control of each information asset node of the cloud business platform, unified security audit management and identity authentication management. The Cloud Services Security Management Center needs to have the following functions.

1) centralized control of user identity authentication, access control and security audit can be achieved, which is an important means to ensure the effective implementation of trusted communication environment in cloud services.

2) the centralized management and scheduling of cloud service resources can be realized, and the flexible resource allocation of cloud services has been separated from the restrictions of physical devices. The centralized management of resource pool can maximize the resource utilization efficiency and dynamic security scheduling capability of cloud services.

3) the unified management of security policy and configuration can be realized. Security policy is the benchmark to realize the security capability of the system, and all devices, services and controls are based on the policy. The security boundary of cloud service is dynamic and changeable, so it is necessary to realize the unified configuration and management of security policy, and effectively realize the optimization and modification of security policy and the division of levels and permissions.

4) it can realize the centralized monitoring and log management of the service system, and help the cloud service system to improve the sustainable service ability.

5) it can achieve efficient emergency response capacity, and can realize the ability to control security risks with a unified standard. Improve the ability and efficiency of handling security incidents.

6) the security management center itself is under the high-level internal security

protection policy, so it can realize the dual protection mechanism for all aspects of security operation and maintenance management and improve the overall security of the system.

Under the unified management framework of the Cloud Service Security Management Center, CoffeeBlend still needs to improve the following details for the discovered data security management problems.

1) develop requirements for the identification and classified management of information assets, especially the management of software and data assets.

2) perfect the management standard of loophole sweep, define the cycle and treatment time limit.

2) improve the management requirements for viruses and malicious code.

3) further improve the ability of system monitoring.

5) introduce third-party security institutions to evaluate the operation and maintenance capacity on a regular basis.

4.4 Identify the level of information assets for classified and hierarchical protection

In the process of protecting the company's information assets, the relevant workers must first figure out what belongs to the security system and policy to protect the object, if the protection object can not be identified, then in many, strong security measures can not play a role. Specifically, its information assets mainly include the following forms: such as services, software and hardware, and many other aspects. most of the different information assets have very sensitive data, which encounter hacker intrusion, data leakage, loss and so on. will bring great negative effects to the company. Because CoffeeBlend's employees and customers are allowed to use their personal devices to access the company's network / resources, and billions of dollars worth of intellectual property rights are also accessible, confidentiality priorities must be given to the information. distinguish intellectual property information from user information.

In the process of protecting information assets, companies first need to identify information assets and classify them on this basis. According to the guiding ideology of IS027001 to identify information assets, information assets mainly include three indicators: integrity, confidentiality and availability. The information assets of CoffeeBlend mainly include the following types:

(1) Top Secret. That is, CoffeeBlend only specific, very little personnel understand, and has a very great commercial value, without the authorization of the company leadership or leakage will greatly affect the benefit of the company and healthy and sustainable development of the information.

(2) Confidential. That is, the company outsiders are often unable to understand, with more or less commercial value, without the leakage or use authorized by the relevant units of the company, the information that will affect the operation of the company or the interests of employees within the company to a great extent.

(3) Internal public class. That is, the information that the company can not disclose to the public, leaking or using at will will have more or less adverse effects

on the company or employees.

(4) external public class. That is, the information that company have spread through public places can be obtained by the broad masses of people free of charge, and this kind of letter. The leakage of interest does not pose a threat or negative effect to employees and the company.

According to the principle of classification and classification of information assets, fully considering the specific business model of CoffeeBlend, the information assets of CoffeeBlend are classified and several representative classifications are shown in the form of tables, as shown in the Table 2-2:

Secrecy level	Description	Example	Influence level
Top secret information	There are only a few specific employees in the company, and it is of great commercial value. At the same time, the use or leakage of information without the authorization of the enterprise leadership will greatly affect the benefit of the enterprise and its healthy and sustainable development.	Overall corporate strategy, future investment strategy, minutes of board meetings, undisclosed financial statements, billions of dollars worth of intellectual property, etc.	Significant
Confidential information	Those who are often unable to understand by outsiders have more or less commercial value. At the same time, the leakage or use without the authorization of the relevant units of the enterprise will affect the operation of the enterprise or the interests of employees within the enterprise to a great extent.	The company's business plan, information about high net worth customers, information about critical financial products in the market, internal management steps, sensitive information, etc.	Serious
Internal disclosure	The information that cannot be made public by an enterprise will be leaked or used at will, which will have more or less adverse effects on the enterprise or employees.	Internal memo, address book, meeting minutes, etc.	Limited
External disclosure	The information that enterprises have spread through public occasions can be obtained free of charge by the broad masses of people. at the same time, the leakage of this kind of information does not threaten the vast number of employees and the company.	Published financial reports, annual reports, information published on the official website.	None

Table 2-2 CoffeeBlend Classification of Information Assets Classification

5 Research significance of updating regulations and standards

5.1 Social significance

The speed of the development of the Internet is far beyond imagination. Today, network services have gone deep into all aspects of social services and daily life, all kinds of massive data and sensitive information are flowing in cyberspace. The security and credibility of network services and information data are becoming more and more influential and harmful to national security, social stability, maintenance of public interests and so on.

Therefore, constantly update the laws and regulations and standards of information security management under the new technology environment, combined with the effective implementation of company goals, effectively improve the comprehensive management and control ability of network security of companies in the new technology environment, for the national macro network security and stability, it has extensive social significance to ensure the healthy and orderly development of economy and people's livelihood.

5.2 Practical significance

For Internet service companies, the new information technology represented by cloud computing technology has brought about too great changes, which is completely different from the traditional business from the aspects of technology, architecture, service model, security boundary, asset management and so on. Personal information protection and mass information data security have great influence and harm to society and companies, and companies are facing great pressure of development. If the laws and regulations and standards of information security management under the new technology environment can not be updated in time, companies will be eliminated by industry and policy laws. In the face of these potential risks and problems, Internet companies need to have a clear understanding from the level of awareness and management. It is urgent for companies to find and improve safety management problems through effective measures and methods from a strategic point of view, so as to avoid hitting the rocks on the waterway where the future business tells the development.

By updating the regulations and standards of information security management under the new technology environment, defining the objectives of information security management, ensuring compliance requirements, and using network security level protection standards to guide companies to improve the construction of information security management strategy. Take the information security technology as the basic means, pay attention to the security strategy and strategy, implement the overall thinking concept of the system, and start with each link of the information security, so as to realize the improvement and optimization of the security management of the cloud service information system.

6 Conclusion

This paper draws lessons from the study of the Information Technology Infrastructure Library (ITIL) and security model examples as well as the ISO 27000 framework. Help CoffeeBlend to rebuild the information security system suitable for

cloud computing services. The future Internet will rely on the integration and expansion of cloud computing technology, mobile Internet technology and big data technology, resulting in a diversified development pattern, bringing rich and colorful products to serve every corner of social life.

It is necessary to continuously explore and develop in the field of information security under the guidance of international security policy and according to unified and advanced security management standards, so as to realize the overall security of the macro network. Internet service companies as an important cornerstone of the current network services, on the one hand, they should quickly adapt to the development of technology and business, and provide support for Internet service experience. On the other hand, it is necessary to effectively control the rapidly changing network security risks.

Through the carding and study of the latest regulations and standards, this paper discusses the effectiveness of constantly updating laws and regulations and standards for the implementation of network security management and control of new information technology. It is hoped that it can help CoffeeBlend to improve its information security management ability, identify new business security risks and implement effective security control.

References

- [1] International Organization for Standardization. (2013). *ISO/IEC 27001: 2013: Information Technology--Security Techniques--Information Security Management Systems--Requirements*. International Organization for Standardization.
- [2] Dimitrios Z, Dimitrios L. Addressing cloud computing security issues[J]. *Future Generation Computer Systems*, 2012, 28(3): 583-592
- [3] Tan C, Liu K C, Sun L. A design of evaluation method for SaaS in cloud computing [J]. *Journal of Industrial Engineering and Management*, 2013. 6(1): 50-72
- [4] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing[J]. *Journal of Network and Computer Applications*, 2011, 34(1): 1 -11
- [5] Ross, R., Katzke, S., Johnson, A., Swanson, M., & Stoneburner, G. (2008). NIST SP800-39, managing risk from information systems an organizational perspective. *Gaithersburg, MD: NIST*, <http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf>.
- [6] Boehmer W . Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001[C]// *Second International Conference on Emerging Security Information*. IEEE Computer Society, 2008.
- [7] Beckers, K., Heisel, M., Solhaug, B., & Stølen, K. (2014). ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system. In *Engineering Secure Future Internet Services and Systems* (pp. 315-344). Springer, Cham.
- [8] Achmadi, D., Suryanto, Y., & Ramli, K. (2018, May). On developing information security management system (isms) framework for iso 27001-based data center. In *2018 International Workshop on Big Data and Information Security (IWBIS)* (pp. 149-157). IEEE.
- [9] Warkentin M, Willison R. Behavioral and policy issues in information systems security: the insider threat[J]. *European Journal of Information Systems*, 2009, 18(2): 101- 105.