

Research on mainstream information security model and case study of CaribbeanCoffee's information security system construction

Yizhen Ma^{1,2}

1.University of Wales Trinity St David, Swansea, Britain; 2.Wuhan University of Technology, Wuhan, China

Abstract: With the rapid development of contemporary information technology, a series of changes have taken place in the social environment. The application of IT in enterprises is becoming more and more extensive, and the degree of business dependence on IT is getting higher and higher; but with it, problems arise such as huge IT investment scale and increasing IT risks. The good operation of an enterprise depends on the understanding and application of information system security principles, while traditional information technology security methods cannot fully keep up with the mission of the times; in addition, due to the information security environment of each company is unique, the existing IT security model cannot be fully applicable for the security needs of every enterprises. In this paper we research several mainstream IT security frameworks and models, analyzes their advantages and disadvantages, draws on their methods and concepts, and proposes an approach based on the ISO/IEC 27001 standard to meet the need of the company information system security according to the given scenario.

Key words: InfoSec; security frameworks and models ; ISO/IEC 27000 series

1. Introduction

Currently, the security of information systems is now very important to prevent from an attack, besides that low security can threaten the productivity of an organization[7]. IT companies are the collection and distribution centers of information resources. With the expansion of business capabilities and the acceleration of their digitization process, how to effectively manage a large amount of information troubles every manager. Information security has become an important issue that every IT company needs to solve. However, at present, many enterprises "emphasize technology and neglect management" for information security, and the construction of information security management system is even more blank. Most enterprise managers have insufficient awareness of the seriousness of threats to information assets, and lack clear strategic planning of scientific information security, systematic information security management system, and relatively effective management measures, etc. Management is the foundation of information security. For IT companies, how to establish a complete and standardized information security management system to standardize information security management, control information security risks, and improve information security defense capabilities is the basis of the next strategic arrangement.

The organization of this paper is as follows, in the second chapter, we research some mainstream frameworks and models of information security, we explore the development history of each framework, analyze the advantages, disadvantages and applicability of them and compare between them. In the third chapter, we propose an approach to establish a complete and standard information security management system for the given scenario to standardize information security management of that company based on the ISO/IEC 27001 standard.

2. Security Frameworks and Models

2.1 COBIT

Control Objectives for Information and Related Technology (COBIT) was created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992 for information technology (IT) management and IT governance. series of generic

processes defined in COBIT aim for managing IT. Each process defined in COBIT accompany with proposal about how to deal with inputs and outputs, and also key process-activities, process objectives, performance measures and an elementary maturity model[1]

COBIT contains 5 components: Framework, Process descriptions, Control objectives, Management guidelines and Maturity models. Framework defines how to combine IT governance goals and valid practice more effectively through IT processes, thus meet the requirements of business goals. Process descriptions define a reference process model and common language applicable to everyone in the organization. Control objectives provides a complete set of high-level goals, which allows managers to consider how to effectively control each IT process. Management guidelines help managers understand how to assign responsibilities to achieve goals, and how to measure performance of each process, at the same time interpret the internal relationship with other processes. Maturity models help evaluate the performance of each process and help to draw the limitation.

COBIT 5[2] which was released in 2012, provides five principles focused on the governance and management of IT in an organization, they are Meeting Stakeholder Needs, Covering the Enterprise End-to- End, Applying a Single, Integrated Framework, Enabling a Holistic Approach, Separating Governance from Management.

In 2018, The updated COBIT 2019 structure and content have new explanations. The new changes are roughly as follows:

(1) Design factors: More factors driving design are introduced, which can promote the design of corporate governance systems (for example, corporate strategy, risk status, IT roles, IT deployment methods, threat factors).

(2) Governance components: The corporate governance system consists of different types of components which must work together as a whole, which is greatly simplified compared with the supporters of COBIT 5.

(3) Key areas: The key areas guidelines will be applicable to information security, information and technology risks, small and medium-sized enterprises and DevOps, and more possible, feasible and planned. A detailed description of these changes can be found in the COBIT 2019 framework.

For the comparison between COBIT and other frameworks such as COSO and FISCAM(Federal Information System Controls Audit Manual). All of these standard frameworks are issued by different countries, organizations, and institutions, and also their applicable fields are different. But all these international standards are consistent to a certain extent. For example, the main focus of these guidelines is on control, security, and services. COBIT is good at learning and drawing on the advantages of existing relevant standards in the industry, focusing on the combination with other standards. Among them, the standard perspective of FISCAM and COBIT are relatively close, both are aimed at the control aspect of information systems. FISCAM includes general control and application control. COBIT has more general risk-based IT control, IT services, information security and internal control[9]. At the same time, it pays more attention to continuously learning and absorbing other international advanced standards and methods, which achieve improving and optimizing its own structure with its own standards, so as to improve the COBIT standards such as risk-based IT general control, IT services, information security and internal control. In addition, the COBIT standards allows different users to creatively combine COBIT with other international standards according to their own needs, so as to better achieve

compliance goals, especially those related to information systems. In short, COBIT has the advantages of having generally recognized good practices in IT governance, and it is also the synthesizer of IT governance, IT security related standards and concepts.

There are also some shortcomings of COBIT, for example, lacking division of relative importance. COBIT adopts a hierarchical structure, based on this, IT processes are divided into 4 domains: planning and organization, acquisition and implementation, delivery and support, and monitoring; 34 processes, although the 34 information technology included in COBIT 4.1 Process control, domain and process are divided in detail, but the drawback is that the COBIT division does not provide the respective criticality between each domain and each process, as well as the relative criticality between domains and processes. Another problem of COBIT is lacking of quantitative description. COBIT focuses on qualitative, while such framework often lacks quantitative description. The COBIT standard provides guidelines for management methods, including: maturity model, key success factors, and key target indicators. In order to better achieve corporate strategic goals, it is very important to efficiently integrate corporate control information systems and business process related processes. But from a quantitative point of view, such a qualitative control framework lacks a quantitative description.

2.2 ISO 27000-series

The ISO 27000-series comprises information security standards are published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [3]. The standards provide guidance on the construction of the Information Security Management System (ISMS), cover issues such as information protection, confidentiality, and IT technology security, and is applicable to organizations of all sizes. The standard system formulates new standards related to information security management every year. Among many standards, the ISO/IEC 27001 standard first proposed the concept of an information security management system, which is the core of the entire ISO standard series.

We compare ISO/IEC 27001 with other mainstream IT security frameworks such as National Institute of Standards and Technology(NIST) and COBIT.

The NIST framework was built by The U.S. National Institute of Standards and Technology. In this framework, the target of management is network communication architecture and equipment related to critical infrastructure. NIST describe information security requirements in five stages of identification, protection, detection, response, and recovery, with dynamic detection of security issues as the main idea. It suits for systems for specific requirements, such as energy, power and other key enterprises. We have analysed COBIT framework in previous section, as we discussed above, COBIT is process-oriented, the major concern of COBIT is information system governance and offer related good practices. which makes it suitable for information system security governance work.

In comparison with these security standards, the ISO/IEC 27001 standard focuses more on the role of management in information systems and describes more management-related scenarios [8]. It involves more management system establishment requirements and focus more on the continuity of business and the integrity of the management system which lead to a favourable adaptability to enterprises with different structures.

2.3 Information Security Level Protection Management Measures(China) and Cybersecurity Law of the People's Republic of China

Information Security Level Protection Management Measures was published by the Ministry of Public Security of China in 2007, it defines the “prescribed actions” that need to be completed for graded protection, namely grade filing, construction rectification, grade evaluation, and supervision and inspection which marks the official launch of Grade Protection 1.0 in China. After that, in 2017, The Cybersecurity Law of the People's Republic of China, commonly referred to as the Chinese Cybersecurity Law, was enacted to increase data protection, data localization, and cybersecurity in the interest of national security[4]. Both of them starting from the information security level of the country and society, constructing an overall national information security analysis level management and guarantee system, which is applicable to Chinese enterprises that involve a certain degree of information sensitivity and have certain requirements for information security.

3. CaribbeanCoffee Scenario

CaribbeanCoffee is an international company which sells Blue Mountain Peak coffee from Jamaica, most of its network is wireless based and the company uses cloud services to deliver IT services to its staff and clients, due to its large staff and international customer base, this company urgently needs a robust information security system to solve the problem of personal privacy protection of employees and customers, as well as the company’s intellectual property protection.

In view of the actual situation of the company, we consider establishing an information security management system suitable for the enterprise based on the ISO/IEC 27000 series for the following reasons. First, ISO/IEC 27000 series are general standards, and adopt the general framework of international standards with good compatibility and easier integration with other management systems, which makes it universal for all industries, Second, The ISO/IEC 27001: 2013 standard regards information as an organization’s asset, and believes that it plays a key role in the survival and development of the organization. It must identify information assets and assume responsibility for protection, and requires information security risk management to focus on information. For CaribbeanCoffee, its day-to-day business is closely linked to information security, so it is in line with ISO/IEC 27001: The 2013 standard has a natural connection and compatibility.

3.1 Information security strategic planning

Information security strategic planning is formulating plan executed by a company in a period of time (generally no more than 5 years) with overall, hierarchical, coordinated, and relatively stable plans. It is the overall idea of the information security development of the company and also the guidance basis for information security management. The information security strategic planning of CaribbeanCoffee(latter will be referred to as the company) needs to consider the following factors, as shown in Figure 1.

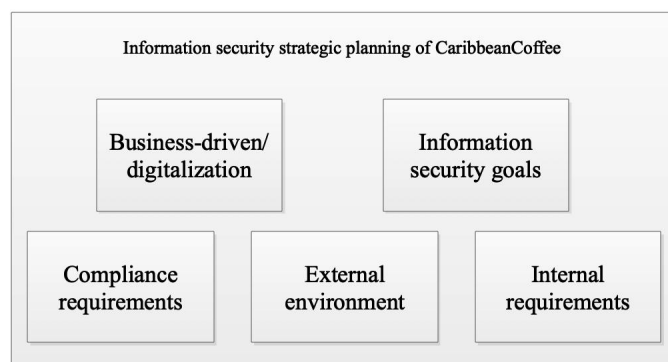


Figure 1. Influencing factors of CaribbeanCoffee's information security strategic planning

- 1) **Business-driven/digitalization:** Based on the company's business development goals and development plans, to ensure consistency with the goals of the company development plan. This is the starting point and also the final point of the information security management plan. Around this theme, the company should realize the top management's commitment to information security and define the mission of information security management, objectives and management methods, and based on the development of physical security strategy, operational security strategy, department communication security strategy, asset security strategy, risk control strategy, emergency response strategy, human resources security strategy, etc. Development plays the role of escort
- 2) **Information security goals:** In ISO/IEC 27001: 2013, it is clearly stated that the goal of an information security management system is to ensure the confidentiality, integrity and availability(C.I.A) of information assets through the application of risk management processes, and to give relevant stakeholders that risks have been fully managed Confidence[5]. This stakeholder refers to both the users where the company is located, as well as those contractors and database vendors that have direct or indirect contact with the company. In addition, consideration should also be given to: ① Establish contact with and maintain consistency with information security strategic planning; ② Balance cost and information security objectives; ③ Information security risk prediction, identification and application of control measures; ④ Performance evaluation can be used to measure the effectiveness and operability of information security goals.
- 3) **Compliance requirements:** This is the control target requirement of ISO/IEC 27001: 2013. It mainly requires that the information security strategic planning of the company and subsequent plans, strategies, implementations, operations, etc., must be consistent with national laws, regulations and policies. Keep the rules and regulations, rules, etc. Consistent and ensure that the relevant procedures meet these requirements in the implementation of information security in the future[5].
- 4) **External environment:** The external environment is also an important factor affecting the strategic planning of information security of a company, and because of its complex composition, the impact on the company is both good and bad, and it is difficult to control. Considering the composition of the external environment, it mainly includes the following aspects: ①The changes of informatization in the company, including the update of informatization planning, the formulation of informatization-related policies, the purchase of

informatization equipment, the information security environment, etc.; ②the emergence of information security related new security technologies, new threats, new systems, etc.; ③ changes in users' information security awareness and skills; ④ changes in the policy environment. ⑤ accidents, such as lightning strikes, earthquakes, fires, long-term power outages, and network outages.

- 5) **Internal requirements:** Information security is the overall requirement of the company, and its information security strategy plan should also be considered from the overall situation of the company. First of all, it is necessary to establish an appropriate balance point to ensure that the company invests the least funds within the acceptable range of information risks; Secondly, it is necessary to consider the needs of the business development of various departments in the company for information security and the priority of the needs; Third, the management, education, training of human resources in the company and the establishment of related systems for information security management should be considered.

3.2 Information security organization structure

The information security management system involves all aspects of a company. From ordinary employees to managers, they are all responsible for information security management. We design a relatively complete information security management organization structure of the company includes the following aspects, as shown in [Figure 3](#).

- 1) **Decision-making level:** Mainly refers to the company's information security leadership group, which is the top-level design and overall planner of the company's information security management work, and is led by the leader responsible for the company's information security construction or specific information security (i.e. chief security officer, CSO), This may include other leaders in the company and individual department heads. The decision-making level is mainly responsible for the planning of information security strategies, the formulation of information security management strategies, the establishment of information security management organizational structure, and the assignment of information security personnel responsibilities.
- 2) **Management level:** It is composed of the heads of the company's information security management department and other department heads. It is mainly responsible for the formulation of the company's information security work plan and policy, the formulation of daily information security management systems, documented operating procedures, information security incident management, and information risk prediction, control, supervision and audit of various departments, information security work implementation, etc., directly report to the chief security officer.
- 3) **Auditing level:** this level consists of hired information security experts, CSO, employee representatives, and customer representatives. It is mainly to establish the company's internal audit system, audit standards, audit methods and audit procedures, formulate audit plans, and regularly review the operation of the company's information security management system. The results of the audit should be linked to the company's staff's assessment to improve staff awareness of information security and standardize the information behavior of employees. At the same time, consider establishing the company's BCP/DRP mechanism, and information security emergency response mechanism, etc., to establish and improve the company's business continuity management framework[6]

- 4) **Executive level:** It is composed of employees from the company's information security management department and other departments responsible for information security. The employees in the information security management department mainly include computer room administrators, network and server administrators, database administrators and information system administrators. The executive layer is an employee team that implements the company's information security plan, implements various information security strategies, comprehensively conducts daily information security management, security service support, security incident control, and information security regulations; especially the information security officers of various departments, who are also responsible for their department's information security rules establishment and information security training, etc. The executive layer is the middle layer that guarantees the full implementation of the company's information security measures, and promotes the continuous improvement of the information security management system itself through continuous practice.
- 5) **User level:** Based on the principle of least privilege, the company can adopt the method of "authorize according to users and exercise rights according to requirements" to realize the information security management of users. That is, according to the level of user information requirements, different systems, resources, services, etc. are granted access and utilization rights. In addition, information security education, training, publicity, activities, etc. should also be adopted to continuously improve users' information security quality and enhance users' conscious standardization of information behavior.

3.3. Information Asset Management

The basis for the company to implement an effective information security system is the identification, management and protection of information assets, so as to improve the company's overall information security management level and avoid information risks in time. A company's information assets can exist in many forms, including intangible information assets and tangible information assets. Tangible information assets also include hardware, software, data, files, etc. Information asset management includes the identification, hierarchical management, periodic management and recording of various information assets.

Information asset identification: confidentiality, integrity and availability of information assets are recognized as three elements that can reflect the security characteristics of assets. The identification of assets is the process of 1) information asset collection; 2) information asset identification; 3) information asset classification; 4) information asset assignment. The identification of information assets is of vital importance to the entire information security management system. Following the principle of minimum disclosure, the company should divide information assets into five levels: top secret, confidential, secret, internal expose, and external expose. By assigning different security levels to different information assets, different management, access, service, and storage strategies are implemented to ensure the information security while providing services as much as possible.

Periodic management of information assets: Periodic management is mainly the management of physical information assets and software information assets. It refers to the entire life course from the needs of physical information assets and soft information assets, from research, analysis, procurement, installation, use, maintenance, replacement to elimination. Through the implementation of full periodic management of information assets, it is possible to effectively

monitor the operating status of information assets, the reliability and economy of information assets, and while achieving the goal of reasonable and optimal utilization of information assets, it also takes into account the development, design, and development of information software assets. Update, technical update of information hardware assets and equipment replacement, etc.

Information asset records: The records of information assets should include the information records required by ISO/IEC 27001: 2013 and the document information that is effective and necessary for the information security management system of a company. Various factors such as the scale, complexity, activity type, process, service and personnel capabilities of the information security management of the company determine the level of detail of information asset records. From the perspective of safety and suitability, the company should make clear information asset records during the process of distributing, accessing, retrieving, using, storing, modifying, and disposing information assets.

3.4 Information security risk assessment

Risk identification: risk identification is the primary step of information security risk assessment. It refers to the use of a systematic method to identify the potential risks hidden in the information assets of the company, at the same time rank the priority of all risks, and identify the significant risks. Risk identification is a complex process, which includes information asset identification, threat identification, weak point identification, and confirmation of existing security measures. Every steps are indispensable for information security risk identification. Often a certain information asset may face multiple threats or the security threats faced by different information assets have their own uniqueness, which requires detailed carry out ISO/IEC 27001: 2013 standard requirements and thorough analysis of information assets, scientific statistical analysis of the probability of threats, and the losses caused after they occur.

Risk evaluation: After identifying the information security risks, the company must assess the potential consequences that the information risks may cause, assess the actual possibility of the occurrence of the risk, determine the risk level, compare the risk analysis results with the established risk criteria, prioritize the entire information and make sure the security risk assessment process is documented. In the process of company risk assessment, quantitative analysis methods can be used, such as factor analysis, cluster analysis, etc.; qualitative analysis methods can also be used, such as factor analysis, logical analysis, etc. It is also recommended that the company combine both quantitative and qualitative methods.

Risk treatment: After the risk assessment, risk treatment should be carried out. Risk treatment must first consider the results of the risk assessment and adjust the risk control plan against the risk treatment plan that has been drawn up; secondly, according to the principle of balancing control expenses and information risk, the main principle of reducing risk for different information risks is to reduce them. The following risk reduction methods can be appropriately selected: avoid risks; transfer risks; reduce risks; reduce weaknesses; reduce the possible impact of threats; detect information security incidents, respond to them and recover. Thirdly, in accordance with the requirements of ISO/IEC27001: 2013, appropriate measures are selected from 114 control measures to reduce the risk. Finally, document the information security risk handling process.

3.5 Information security protection management

As information security issues become increasingly prominent, information security protection has

also become the focus of every company, which is also a requirement of the ISO/IEC 27001: 2013 standard system. According to the actual situation of the company, here we propose several practical strategies to achieve information security protection of the company.

- 1) **Choose appropriate cloud.** Users must first conduct risk assessment and analysis on enterprise data and application services. Public cloud services can be used for general services that carry public information, especially those services that have low utilization, high maintenance and upgrade costs, and low correlation with other systems should give priority to public cloud services. For important services that carry sensitive information, private clouds with better security characteristics are preferred. Systems that carry key services are not suitable for public cloud services, private clouds should be considered. When choosing a cloud service provider, the company should choose a qualified cloud service provider, and the cloud platform it provides should have the security protection capabilities corresponding to the level of the information system, agree on the cloud service provider's authority and responsibilities, and agree when the service contract expires, Return information, clear data, sign confidentiality agreement, provide operation supervision interface, etc.
- 2) **Security authentication,** unified and centralized security authentication should be established to meet the complex user authority management of multiple users and a large number of access authentication requirements in the environment, at the same time improve the security of user identity management and authentication in cloud services. Specifically, single sign-on authentication, mandatory user authentication, and a combination of authentication between different security domains can be used. By combining mandatory user authentication and single sign-on authentication, the user is allowed to enter the service authentication, and the user can enter the application with only one identity authentication, thereby effectively reducing the risk of password leakage.
- 3) **Data encryption,** in order to ensure data security, data encryption technology should be used to encrypt data, which can effectively ensure data security. Nowadays, well-known cloud service providers on the market all encrypt data with different algorithms to ensure the confidentiality of system data.
- 4) **Data backup,** using data backup to ensure data security is a common data protection method. Some cloud service providers have automatically provide their customers with data backup or redundancy functions. Some of them have established multiple data centers to replicate data to ensure data security. In addition, some cloud service providers use redundancy and backup plans to provide high system availability even when system downtime.
- 5) **Access control,** service providers and enterprises should provide different permissions to guarantee data security. Enterprises should have complete control authority and restrict authority to service providers. The responsibility of the cloud service provider is to design an identity access management strategy, which covers not only the cloud platform, but also the applications and services presented to the outside world. Access rights should be based on granting user rights on the basis of "lowest rights", rather than giving everyone more rights. This can improve auditing capabilities and reduce the risk of unauthorized changes to platform data.
- 6) **Secure transmission,** The problem of network transmission security can be solved by encrypting the transmission content. Data is transmitted to the cloud through the network. In

order to ensure the security of data transmission, SSL, HTTPS, VPN, etc. are used in the transmission process, and the data is transmitted in cipher text.

4. Conclusion

In this paper, we research current mainstream information security frameworks. Based on their comparative analysis and the scenario, we propose an approach to establish a complete and standard information security management system for the given scenario to standardize information security management of that company based on the ISO/IEC 27001 standard.

In accordance with the new international information security management standards, building an information security management system to resolve information security risks is the immediate need and a long-term plan. ISO/IEC 27001 provides a relatively complete set of information security control objectives and control measures, but how to combine these control objectives and control measures with the actual business work of actual scenario and how to implement it to meet the development needs of one company needs more in-depth research.

References

- [1] Haes, S.D.; Grembergen, W.V. (2015). "Chapter 5: COBIT as a Framework for Enterprise Governance of IT". *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5* (2nd ed.). Springer. pp. 103 – 128. ISBN 9783319145471. Retrieved 24 June 2016.
- [2] "COBIT 5 for Information Security". ISACA. Retrieved 24 June 2016.
- [3] Information technology-Security techniques-Information security management systems-Overview and vocabulary ISO/IEC 27000[S].2014.
- [4] Wagner, Jack (2017-06-01). "China's Cybersecurity Law: What You Need to Know". *The Diplomat*. Archived from the original on 2018-12-12. Retrieved 2018-12-14.
- [5] ISO/IEC 27001: 2013.Information Technology—Security Techniques—Information Security Management Systems—Requirements[S].Geneva: International Organization for Standardization, 2013.
- [6] Zhu Xuan. Research and implementation of information security management system based on ISO 27001[D]. Shanghai: Shanghai Jiaotong University, 2009: 5-11.
- [7] Prapenan G G , Pamuji G C . Information System Security Analysis of XYZ Company Using COBIT 5 Framework and ISO 27001:2013[J]. *IOP Conference Series: Materials Science and Engineering*, 2020, 879(1):012047 (6pp).
- [8] Zhu Xuan. Research and implementation of information security management system based on ISO27001[D]. Shanghai: Shanghai Jiaotong University, 2009.
- [9] Zhao Lei. Research on A Hotel IT Governance Practice Based on COBIT Framework[D]. 2018.