

Construction of IT framework and model to solve the problem of information leakage in Caribbean coffee

Yachao Li

Abstract

With the rapid development of the Internet, people are inseparable from work and life. However, while people enjoy all the conveniences brought by the network, computer network security has become a highly concerned problem. As we all know, if there are security problems in the computer network, it will not only make people's private information leak, but also cause certain losses to the enterprise. Based on this, this paper will take the current situation of computer network security as the starting point, and focus on several targeted frameworks to solve computer network security problems. According to their different roles, there are divided into security control framework (SCF), security management plan (SMP) framework and it governance framework (ITGF). And choose the appropriate framework to solve the information security and management problems of Caribbean coffee.

Keywords: Data security; IT infrastructure library ITIL; ISO 27000; IT Security; COBIT framework.

1. Introduction

With the rapid development of China's science and technology and information network technology, the computer has become the most important tool for us to obtain information, and the application of computer network has gone deep into all aspects of enterprise work. For example, some banks use online securities trading system to trade with customers; some technology companies need to use the Internet to communicate with global customers; some online shopping companies and machine learning related companies need data analysis to solve problems and formulate future development strategies.

More importantly, each company has its own high-quality data and confidential information. Most companies have opened social network pages, there are more access points, such as the flow of employees, replacement and increase, so all kinds of new and old security problems always exist in the enterprise. If the enterprise's drawings and source code, business and other core data leak, the enterprise as a whole must bear the risk, the most direct is the economic loss. The information leakage of enterprises will also lead to the decline of the prestige and trust of enterprises in the public, which will directly change their original choice tendency. Therefore, information leakage events may make enterprises lose a large number of existing or potential customers. Therefore, it can also be said that in today's increasingly

important role and status of data information, the security of data information is related to corporate reputation, public trust, economic interests, life and death. The security degree of enterprise data information will affect the external competitiveness of enterprises.

In order to protect enterprise information and reduce unnecessary losses, in today's globalization, countries or regions and enterprises all over the world need to take corresponding measures to protect enterprise information from damage and leakage. The focus of enterprise information security protection lies in the data itself. As long as the basic data of the enterprise is controlled, no matter how it is transmitted, the security and integrity of the core data information can be ensured, and the loss caused by the leakage and damage of the data information can be eliminated. Generally speaking, to prevent information leakage mainly from the following considerations: mail system, timely communication tools, network tools to prevent leakage; mobile hardware equipment to prevent leakage; business computer to prevent leakage; outgoing data to prevent leakage. In a word, large enterprises need to use the corresponding security model to build a complete set of safe and efficient information management and protection system to ensure the normal operation of the company's business. Employees also need to enhance their awareness of prevention, protect their personal information, abide by the company's laws and regulations, and not disclose the company's business secrets. Multinational companies also need to comply with the laws and regulations of the relevant regions.

This paper describes and studies three kinds of Network Security frameworks and models, and compares them.

2. Security framework and model

This paper studies three security frameworks and models, namely ITIL, ISO 27000 and control objectives of information and related technologies, and compares their commonness, advantages and disadvantages.

2.1 Information Technology Infrastructure Library (ITIL)

ITIL (IT Infrastructure Library) is a set of IT service management standards library developed by CCTA in 1980. It sums up the best methods of IT management from all walks of life in the UK and turns them into norms. It aims to provide a set of standard methods from planning, R & D, implementation to operation and maintenance for IT departments of enterprises. This set of standards has been adopted by many enterprises in Europe, America and Australia. At present, more than 10000 well-known companies in the world are referring to the methods to manage their IT systems.

ITIL's goal is to identify the programs that are really needed by its customers, and these programs are necessary to provide high-quality and most appropriate services at an acceptable cost. There are hardware, software, program, document and personnel to be managed in IT infrastructure. ITIL can be used in part or in whole, and it is very suitable to be used as the basis of management platform.

There are ten important IT management key modules in ITIL. They are configuration management, service desk, problem management, change management, software control and release, service management, capacity management, availability management, accident management and expense management. The ITIL process is shown in Figure 1.

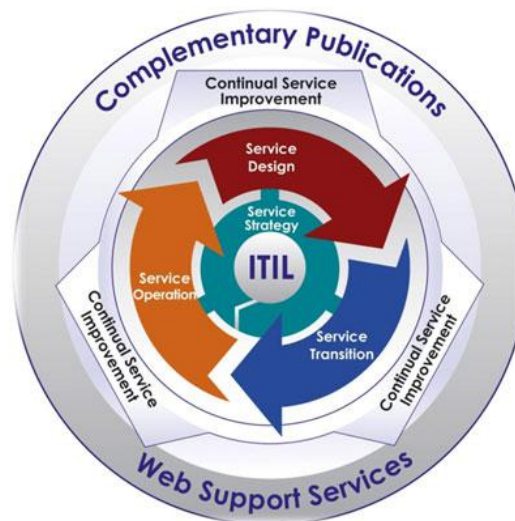


Fig 1. The process of ITIL

2.1.1 configuration management

The purpose of configuration management is to maintain the configuration records of each IT infrastructure in the configuration management database (CMDB). The second purpose is to provide reports of configuration items (CIS). This includes some management information, such as problem records, change records, version information, status information, relationship information, etc.

2.1.2 service desk

The service desk provides daily service window for IT users. Users feedback dissatisfaction with IT services, questions and suggestions, etc. For this reason, the service desk should be an interface window where users can easily give feedback.

The service desk is also the login point for users to use IT services, and their performance represents the service quality of IT services to customers. At the same time, the service desk is also responsible for assisting customers to resume service operation as soon as possible, such as providing guidance, correction, or remedy for an accident. The service desk is not responsible for the analysis of accidents. This

kind of in-depth analysis belongs to the category of problem management.

2.1.3 problem management

The purpose of problem management is to find out and remove the mistakes in IT service, so as to maintain a stable IT service.

2.1.4 change management

The purpose of change management is to ensure that there are standardized methods in the process of IT service changes to effectively monitor these changes and reduce or eliminate the problems caused by changes. The so-called "change" refers to a new state caused by some actions on it infrastructure projects. All changes in configuration items must be brought under the control of change management.

2.1.5 software control and release

The purpose of software control and release is to ensure the security of all software modules, so as to ensure that only the correct version after complete testing is authorized to enter the formal operation environment. In order to control the software version, we must establish a "final software library" (DSL), which may be a physical or logical repository. Either way, it's a place to store officially authorized software versions.

2.1.6 service management

The purpose of service management is to make the service provider and the customer reach a mutually agreed best service agreement at an acceptable cost. This means that service management requires long-term communication between service providers and service recipients. Service management focuses on service standards from a business perspective rather than from an it perspective. Although the long-term end-to-end monitoring report and the utilization rate of each component are important, it is the service quality of the enterprise that is the focus.

2.1.7 capacity management

The purpose of capacity management is to support the best efficiency of IT services, mainly in adjusting the balance between operational needs and it resources. Simply put, capacity management is to ensure that the right resources are provided at the right time, place and cost. It is very important for it department to make effective use of available resources and make plans for the future needs of system operation.

2.1.8 availability management

Availability management is to ensure the availability of IT services under the premise of the correct use of resources, methods and technologies. When enterprises rely more and more on it, in order to maintain competitiveness, it must avoid or reduce unexpected downtime. Availability management in-depth study of those resources and measurement is necessary to maintain the best operating state, hoping to make the

most effective use of resources.

2.1.9 Contingency Management

Accident management is to deal with it crisis and recover from it. For example, it is necessary to transfer the work to another system when it is unable to provide services for a period of time, which should not be met normally. We need to develop a plan to get back to normal operation in the face of it crisis.

2.1.10 Cost Management

Cost management is the cost of providing in-depth understanding, supervision and it recovery operations. This program provides relevant financial information in order to achieve the highest cost performance. It's hard to make a service quality management fee agreement.

2.2 Information Organization for Standardization 27000 (ISO)

ISO / IEC 27000 is the general name of a series of related standards specially established by international organization for Standardization for information security management system. It has reserved 60 standard numbers from ISO / IEC 27000 to ISO / IEC 27059. So far, there are 8 information security management system (ISMS) standards officially released, two of which have been transformed into national standards. All standards, from ISO / IEC 27000 to ISO / IEC 27037, as well as ISO 27799 and others, can be basically divided into the following four parts.

The first part is the requirements and supporting guidelines, including ISO / IEC 27000 to ISO / IEC 27005, which are the basis and basic requirements of information security management system; the second part is the guidelines on certification and audit, including ISO / IEC 27006 to ISO / IEC 27005 27008, for certification bodies and auditors; the third part is the information security management requirements for specialized industries, such as the financial industry, telecommunications industry, or specifically applied to a specific security domain, such as digital evidence, business continuity; the fourth part is the ISO standard which is developed by the ISO Technical Committee tc215 alone (not jointly with IEC) and applied to the health industry 27799, as well as some achievements in the research stage and reflected in the form of new project proposals, such as supply chain security, storage security, etc. Some standards are shown in the attached table. This article will introduce the main standards of ISO / IEC 27000 family.

ISO / IEC 27000 is an overview and term of information security management, which is one of the most basic standards. It provides the general terms and basic principles involved in the ISMS standard family. Because each isms standard has its own terms

and definitions, as well as the differences in the use environment and industry, there are often some subtle differences between the terms of different standards, resulting in the relative lack of coordination in the use process, and ISO / IEC 27000 is used to achieve this consistency. The ISO / IEC 27000 standard has three chapters, the first chapter is the scope of the standard; the second chapter introduces the ISO 27000 series of standards, and explains the relationship between the various standards; the third chapter gives a total of 63 terms and definitions related to the ISO 27000 series of standards.

2.3 Control Objectives for Information and Related Technology (COBIT)

COBIT is an IT governance framework developed and maintained by ISACA. ISACA supports those who want to better manage their overall IT and those responsible for auditing it. For more than 20 years, the framework has been used by organizations that want to strictly manage all areas of IT governance. COBIT, with its main characteristics of focusing on business, process oriented, control based and measurement driven, can connect and control IT and business. COBIT is mainly an IT governance tool, and it can also be used as a guide to establish and improve internal IT control and audit.

With the development of the times, COBIT also has some other extensions, such as the security of governance. In a word, learning COBIT framework is very important for us. “COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT” and “helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use” (ISACA 2012). Figure 1 presents the development of COBIT over the years.

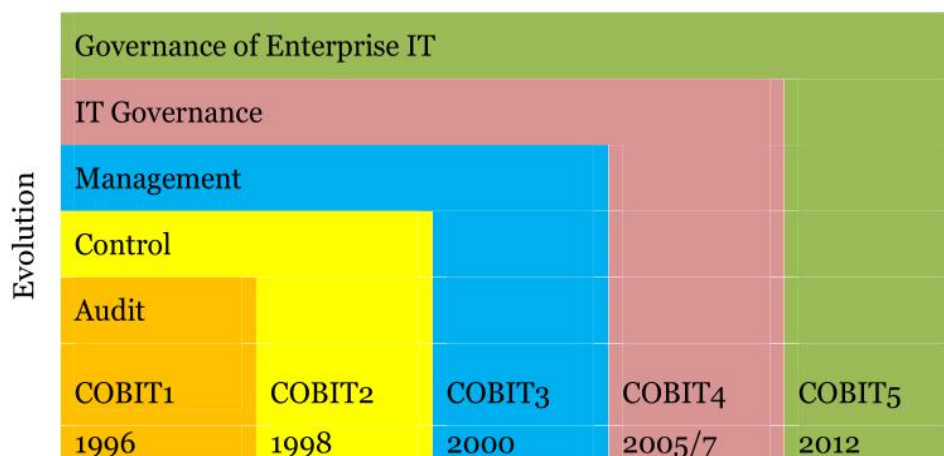


Figure 2. COBIT – The Evolution (Adapted from (ISACA 2012))

2.3.1 Importance of IT governance and COBIT for research and practice

Research on COBIT and the associated IT governance is important due to various reasons:

1. IT is increasingly becoming central to business performance thereby justifying demand for governance (Wilkin and Chenhall 2010).
2. Most businesses still have not established adequate control over IT (Hardy 2006).
3. Organizations face a wide spectrum of external threats arising from IT including abuse, cybercrime, fraud, errors, and omissions (De Haes et al. 2013).
4. Today's enterprises demand a high degree of compliance of business processes to meet diverse regulations and legislations (Elgammal et al. 2014).
5. Ensuring software systems conforming to multiple sources of relevant policies, laws, and regulations is significant because the consequences of infringement can be serious (Tran et al. 2012).
6. One of the most enduring problems faced by the IT function is how it should organize and structure itself (Schwarz and Hirschheim 2003).
7. Growing gap between scholarly research and contemporary practice in IT governance (Sambamurthy and Zmud 2000).

3. Discussion and Comparison

ITIL security management focuses on the process of defining how security works in the context of ITIL, and ultimately defines the controls that may be required. However, it does not provide a list of controls themselves, but a process oriented framework. Focusing on IT governance rather than security, there is a serious tendency towards process control rather than technology control (such as change, asset or event management). Security is regarded as a supplementary issue, while risk management may be closer to the core of the framework.

SCF can be used alone. However, if there is no safety management plan (SMP), the long-term effectiveness and reliability of the control list will be severely limited, and it will be difficult to have a fruitful dialogue with the leadership, and it will be difficult to reach an agreement with the same level team.

ISO27000 belongs to security control framework (SCF) and unified compliance framework (UCF): UCF is a comprehensive (commercial) mapping system, which maps regulations, standards and other control drivers, but it is not an independent framework.

SCF can be used alone. However, if there is no safety management plan (SMP), the long-term effectiveness and reliability of the control list will be severely limited, and it will be difficult to have a fruitful dialogue with the leadership, and it will be difficult to reach an agreement with the same level team.

COBIT is an IT governance framework developed and maintained by ISACA. ISACA supports those who want to better manage their overall IT and those responsible for auditing it. For more than 20 years, the framework has been used by organizations that want to strictly manage all areas of IT governance.

COBIT has expanded over time, introducing other aspects of governance, including security. But its security part is more limited than the SCF framework. Therefore, unless organizations use COBIT as an IT governance method, it is rarely seen that organizations use COBIT to achieve information security.

4. Apply three security frameworks to solve the information security problem of Caribbean coffee shop

Caribbean coffee sells blue peak coffee from Jamaica, one of the best and most popular blends in the world. Caribbean coffee has a wide range of businesses around the world. The company uses cloud services to provide IT services to its employees and customers. It is estimated that almost 95% of the company's networks are wireless based. The company also has a large online and social media business to promote its activities. Due to its large staff and international customer base, the company has been under great pressure recently to require its staff and customers to use their own personal devices to access the company's network / resources. The security of personal employee data and customer data is the main concern of the company. The company is also concerned about protecting its billions of dollars worth of intellectual property. Information security is the top priority of the company, but everything is in a mess. There is no established policy that covers their security needs. Therefore, it is very important to design a stable network security framework for the protection and future development of the company.

The three frameworks should work together, and for most organizations, the security control framework consists almost entirely of a set of controls. However, control by itself does not effectively protect your organization. Like CIS20 and ISO27002, although very popular, but not enough to achieve consistent "good" safety effect.

In order to achieve higher maturity, better efficiency and the ability of measurement and communication, organizations need to use the security management plan (SMP) framework to manage security control. This applies not only to process control, but also to technical control. It's like using CIS.

Finally, 20% of organizations are forced to develop a security management plan (SMP) to provide confidence for the implementation of each of the 20 controls and about 200 sub controls.

IT governance is the security enablers. IT governance framework (itgf) has a significant impact on security. IT governance provides all the foundations for change management, asset management, enterprise planning - that is, security and effectiveness. When an organized security plan coexists with an organized IT plan, it will provide robust security effectiveness.

In summary, by implementing all three frameworks, organizations can benefit from the consistency between security control definition, security governance process, and security and IT governance. When all three framework types work together, you can achieve excellence in the organization and delivery of security. The framework proposed in this paper takes COBIT as the IT governance framework, ITIL as the security management framework, and ISO27000 as the security management plan. The security framework is shown in Figure 3.

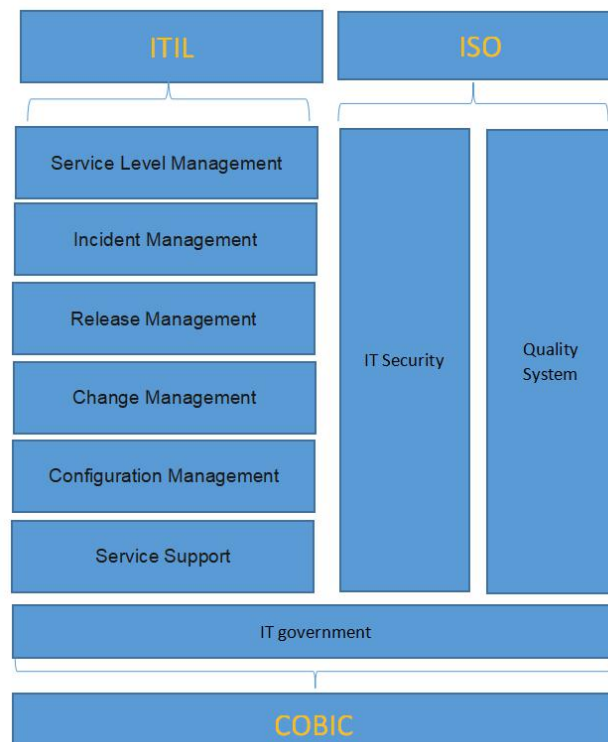


Fig 3. The model of PDCA

4.1 Service Level Management

Service level management is a strict advanced methodology and process, which is the process of defining, negotiating, contracting, testing and reviewing the service quality level provided to customers. It includes problem management, event management, release management, change management, configuration management and service support.

In this framework, different management aspects are set and corresponding to

different service types. It is necessary to realize the ability to monitor the data of the whole company in real time and train and replace the employees. Finally, we need to set up a service evaluation system to get customer feedback in time, so as to improve service quality and service management level.

4.2 IT Security

IT security refers to a series of network security policies used to prevent unauthorized access to organizational assets such as computers, networks and data. With the increasingly cunning means of hackers, the necessity of protecting digital assets and network equipment is becoming more and more prominent. Although the cost of IT security implementation is high, it may cause a greater loss to the organization. Major loopholes may even endanger the normal operation of small and medium-sized enterprises. During or after a security incident, the IT security team can implement the incident response plan as a risk management measure to control the situation. IT security can prevent malicious threats and potential security vulnerabilities. IT security helps to ensure that only authorized users can access and change sensitive information in the network when relevant staff enter the company's internal network. IT security can effectively ensure the confidentiality of organizational data.

4.3 Quality System

Throughout the development history of quality management system, Fagenbaum, the founder of total quality control, defines quality control as "an effective system to coordinate people's quality maintenance and quality improvement efforts in the organization. The system is to produce products that customers are completely satisfied with at the most economic level."

Quality management expert Dr. Deming defines quality management as "to produce the most economical products with use value and commodity, and to apply the principles and methods of statistics in all stages of production."

The definition of "ISO 9000" refers to the quality control system in organization.

In fact, in order to complete a good product or service, all the elements that need to be realized through management activities constitute an organic whole.

The quality management system is built to achieve the quality policy and objectives. The quality management system is to coordinate the people within the organization to achieve the goals of the organization. All kinds of requirements and systems of quality management constitute the whole system. Management is the means to achieve quality objectives.

Quality management system runs through all kinds of organizations Process management of the whole process.

5. Conclusions

Through the introduction of the three network security framework models and the discussion of their advantages and disadvantages, we have a further understanding of the network security framework. Through the combination of three different frameworks, a complete set of information security management system is designed for the information security leakage of Caribbean coffee, which can protect the company's property and comb the information. Network security architecture is also in continuous development. In recent years, there are many different excellent network security architecture models. We should choose the appropriate network security architecture model according to the different needs of different scenarios to achieve the best effect.