

# Apply the principles and practices of Data security, Governance and Compliance based on CoffeeBlend company

Yifei Sun

January 2023

## 1 Abstract

This article conducted research on various security frameworks or models such as the Information Technology Infrastructure Library, the International Organization for Standardization, and other security frameworks. Utilizing the knowledge and understanding gained from this research, a method was designed to address the company's information system security, governance, and compliance needs. Finally, the importance of continuously updating or revising policies, regulations, and standards as good practice was critically analyzed and discussed.

## 2 Related work in literature

1. This paper discusses the application of the IT Infrastructure Library (ITIL) framework in the field of IT governance. The study is based on secondary data and aims to understand the relationship between the ITIL framework and IT governance. The paper also examines how the ITIL framework can assist organizations in managing IT resources, including prioritizing and justifying IT investments, controlling, budgeting, and defining authorization levels. The authors argue that effective management and use of IT services is crucial for modern businesses to improve their performance,

and IT governance helps businesses plan and control IT investments in order to achieve their business objectives. IT governance is a part of enterprise governance that focuses on managing IT resources and prioritizing and justifying IT investments, controlling, budgeting, and defining authorization levels[1].

2. This paper, titled "Methodology for Dynamic Analysis and Risk Management on ISO27001," presents a methodology for dynamic analysis and risk management to help organizations implement the ISO 27001 information security management system standard. The authors describe the design and implementation of the methodology and validate it through a real case study[2].

3. This article discusses the differences between cyber security and information security, noting that while information security considers the role of humans in the security process, cyber security considers this as an additional dimension and also focuses on the fact that humans are potential targets. The article states that such discussions on cyber security are important because they focus on the ethical issues of society as a whole. To address cyber security issues, various frameworks and models have been developed. The article also introduces the concept of cyber security in terms of its framework, workforce, and information related to protecting personal information on computers. The article reviews these models, along with their limitations, and reviews past techniques used to mitigate these threats. The article also provides recommendations for future research[3].

4. This article discusses the challenges and opportunities of cybersecurity in the big data era. The authors first provide an overview of big data and its impact on cybersecurity, highlighting the need for new approaches to secure big data and the emergence of data-driven security. They then discuss various data-driven security techniques, including machine learning and artificial intelligence, and their potential applications in cybersecurity. The authors also examine the role of big data analytics in improving cybersecurity, including the use of predictive analytics and real-time analytics to identify and mitigate cyber threats. The article concludes with a discussion of the challenges and future directions for data-driven security in the big

data era[4].

5. In this article, the author discusses the challenges of securing university networks and data. The author notes that universities have unique security needs due to the large and diverse user base, the high volume of sensitive data, and the open and collaborative nature of academic research. The author also discusses the importance of having a comprehensive security strategy that addresses the various threats facing universities, such as malware, phishing, and insider threats. The author concludes by outlining some best practices for securing university networks and data, including the use of encryption, access controls, and incident response plans[5].

### 3 Introduction to Security Frameworks and Models

#### 3.1 Information Technology Infrastructure Library

Information Technology Infrastructure Library (ITIL) is the most widely used service management framework for helping organizations manage their information technology (IT) services. ITIL includes a set of guidelines, processes, and tools for helping organizations better manage their IT services in order to meet business goals and needs.

The purpose of ITIL is to improve the quality of IT service by providing standard service management processes and to provide a better service experience for users. ITIL consists of five main parts: service strategy, service design, service transition, service operation, and service improvement.

1. Service strategy is the most important part of ITIL, as it lays the foundation for the entire service management framework. The purpose of service strategy is to help organizations develop their IT service management strategy and determine the value, cost, and risk of services.

2. Service design is the part that determines how services will be provided. It covers the design, development, and testing of services.

3. Service transition is the process of moving services from design to the production environment. It covers the deployment, migration, and support of services.

4. Service operation is the part that ensures that services are run-

ning as expected. It covers service monitoring, event management, problem management, change management, and configuration management.

5. Service improvement is the part that continuously improves the service management processes. It covers the evaluation of current service management processes, planning service improvement activities, and implementing improvement activities.

ITIL is widely used in various organizations, including government agencies, financial institutions, healthcare organizations, and retail businesses. Its advantage is that it can help organizations improve the quality, efficiency, and reliability of IT services and provide a better service experience for users.

### 3.2 ISO27000

ISO 27000 is a family of standards related to information security management. ISO 27001 is the main standard in this family, and it outlines the requirements for an information security management system (ISMS). An ISMS is a systematic approach to managing and protecting an organization's information assets, including its data, systems, and networks.

Here is a summary of the main processes involved in implementing and maintaining an ISMS based on ISO 27001:

1. Conduct a risk assessment: The first step in implementing an ISMS is to identify and assess the risks to the organization's information assets. This involves identifying the assets, assessing the likelihood and impact of potential threats, and evaluating the effectiveness of existing controls.

2. Select appropriate controls: Based on the results of the risk assessment, the organization will need to select controls to protect against identified risks. These controls could include technical measures (e.g., firewall, antivirus software), physical measures (e.g., access control), or organizational measures (e.g., policies and procedures).

3. Implement the controls: Once the appropriate controls have been identified, they need to be implemented according to a plan. This may involve purchasing and installing new technology, updating policies and procedures, or training employees.

4. Monitor and review the controls: The effectiveness of the controls needs to be monitored and reviewed regularly to ensure they are still effective in protecting against identified risks. This may involve conducting audits, testing systems and processes, and analyzing performance data.

5. Continuous improvement: The ISMS should be a continuous process of improvement. This involves regularly reviewing and updating the controls in response to new threats, changing business needs, or other factors that may impact the effectiveness of the controls.

## 4 Case scenario analysis

CoffeeBlend is a company that sells Jamaica coffee and has a global presence. It uses cloud services to provide IT services to its staff and clients, and a significant portion of its network is wireless. The company also has a strong online and social media presence. Recently, the company has faced pressure to allow both its staff and customers to use their personal devices to access the company's network and resources, but it is concerned about the security of personal data and the protection of its intellectual property. Currently, the company does not have a established security policy in place.

For this case, the Information Technology Infrastructure Library (ITIL) and the International Organization for Standardization (ISO) security frameworks could be considered to help CoffeeBlend organize its information security management.

Using the Service Strategy section of ITIL, CoffeeBlend could develop a clear information security strategy and determine the value, cost, and risks of its information security services. Using the Service Design section, CoffeeBlend could determine how to deliver its information security services, including the ways in which staff and customers can access the company's network/resources. Using the Service Operation section, CoffeeBlend could implement information security controls to protect the company's data and intellectual property. Finally, using the Service Monitoring and Control section, CoffeeBlend could monitor and evaluate the effectiveness of its information security controls and make improvements as needed.

Additionally, the ISO 27000 series of standards could also help CoffeeBlend manage its information security. These standards provide a common framework to help organizations identify and manage information security risks and ensure the effective operation of their information security management systems.

Overall, using security frameworks such as ITIL and ISO 27000 can help CoffeeBlend organize its information security management, protect the company's data and intellectual property, and ensure the effective operation of its information security management system.

## 5 Security optimization design for CoffeeBlend company

### 5.1 Security requirements for the company's network information system

Before starting the security optimization design for the network information system, CoffeeBlend company needs to have a thorough understanding of its own security requirements and summarize the security requirements for various aspects of the network information system based on the current situation. As shown in Figure 1, a complete risk assessment process is carried out for CoffeeBlend company:

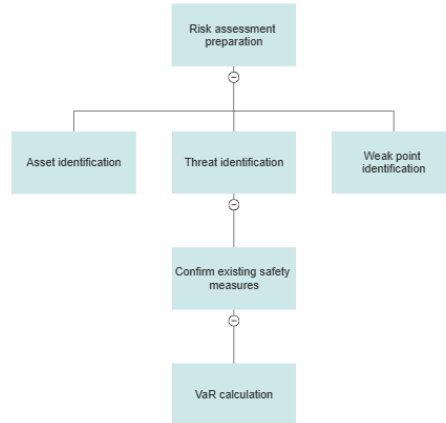


Fig 1: Risk assessment implementation process

First, clearly define the content of security requirements, including security policies, security management systems, resource management systems, management team building, and security protection plans. Second, clearly identify areas that need to be strengthened in terms of security, including intersystems, databases, data transmission processes, virus invasion prevention and defense, security vulnerability detection and audit certification. Then, refine the security requirements for these areas, adjust the structure of the network information system, and improve and upgrade the corresponding security measures. Finally, these security requirements are specific to the actual optimization design process to enhance the level of security protection and the scope of security management, and to ensure the security of the CoffeeBlend company's network information system.

## 5.2 Network information system security optimization goal

The construction of the network information system of CoffeeBlend company has security requirements. Based on the preliminary investigation and analysis, the network information system has been analyzed on a theoretical level, and then various parts have been designed and security optimized at corresponding levels to achieve the desired security optimization goals. The specific content is as follows:

1. It is necessary to detect information access within and outside the network information system, clearly identify the source of access, the content of access, the time of access, and the result of access, to ensure the normal progress of access, and prevent unauthorized and illegal access. At the same time, through effective prevention and management measures, timely discover and report illegal access and abnormal situations during access, in order to ensure the normal progress of company network information system related access activities and protect security.

2. Through the establishment of a real-time monitoring system, increase control over information in the network information system, carry out in-depth analysis of protocols, sources and content of data packets in the network, and timely discover and take corresponding measures to deal with security risks. The objects of monitoring include network devices re-

lated to the system, malicious attacks from inside and outside, database systems and application software, etc., record their running status and report abnormalities. A good linkage relationship between the monitoring system and the security protection system should be established to achieve dynamic monitoring and corresponding processing of security protection.

3. Set appropriate permissions for all users of the network information system, verify the identity of the accessed user, identify its authenticity, and ensure the security of company key documents, programs, data, and other information, to ensure that they are used by legitimate users. During the process of user use, security management is carried out to improve the legality of the use process, improve management efficiency, and further ensure the security of the information.

4. Introduce corresponding security assessment and analysis services, regularly evaluate and analyze the overall information of the company's network information system, timely understand the system to correct vulnerable parts and impacts, and adjust the corresponding security strategy for the optimization of the security system, to ensure the sustained security of the company's network information system, and also facilitate the company's network administrators to strengthen the protection measures of the system in a timely manner, and enhance the professional service and ability of security protection.

5. All security-related states and practices in the network information system can be logged and properly preserved, and a good reading system can be established to carry out log audit work, so that the network information system can be well grasped by the company, understand the situation at any time, and according to the results of log audit, process the corresponding parts of the system to form a good cycle and continuously improve the security performance of the system.

### 5.3 Optimization Design Principles of Network Information System Security

The security optimization of the network information system of CoffeeBlend company should first strictly follow the requirements of relevant

national laws and regulations, and then divide the actual network information system of the company into different parts, including production, office, and external areas, for reasonable isolation and control. The security optimization of the network information system is not independent, and it needs to integrate the network status of various departments and promote the coordinated action of various parts to achieve the design goals.

#### 1. Systematic design principles

The network information system has network hierarchy and integrity, and needs to combine the latest security concepts and security technologies to build a solid system security structure, based on which to establish a complete security system, and use the security system to conduct a comprehensive security risk analysis of the system, timely discover and deal with security problems and hazards in the system.

#### 2. Controllability design principles

The relevant security equipment, technical means, and protective measures used in the design of the network information system all need to achieve the control purpose for security. During the implementation process of system optimization, the progress of the project, human and material input, the effectiveness of security measures, and the quality of network equipment should be effectively controlled to prevent the implementation of optimization from being out of control, resulting in the inability of the company's network information system to achieve the design goals and meet the actual needs of the company.

#### 3. Comprehensive design principles

The optimization design of the network information system needs to consider the impact factors from all aspects, and carry out comprehensive design from hardware, software, network, system and other aspects. Appropriate design principles should be chosen according to the different needs of different areas, and combined with the system security requirements to carry out comprehensive optimization design. According to the degree of security risk and the importance of the information, targeted security protection measures are adopted to design a cost-effective security optimization scheme that improves the interests of the company.

#### 4. Standardization Design Principle

The optimization design of the network information system needs to comply with relevant security management and security standards, and the design results should also meet the principle of standardization for effective implementation.

#### 5. Reliability Design Principle

Security equipment and technology used in the design process of the network information system need to consider reliability, and select technology with a large number of practical cases and commonly used equipment in the market to ensure the stable operation of the design plan after implementation, without affecting the overall use of the company and providing security protection.

#### 6. Simplification Design Principle

The design of the network information system should reduce the implementation difficulty of subsequent plan implementation, the convenience of actual use and the flexibility of management, and the system can simplify the management of relevant security equipment and measures.

Using these design principles, the network information system of CoffeeBlend company is optimized for security design, as shown in the main structure in Fig.2.

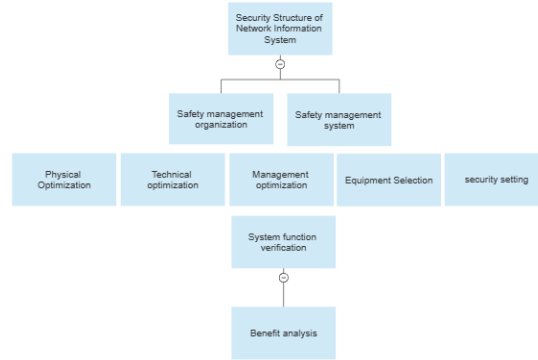


Fig 2: Security Structure of CoffeeBlend's Network Information System

## 5.4 Functional design

1. Authentication method: Use two servers alternately to perform basic hardware configurations, then expand the database on top of the original database.

2. Security level configuration: Configure different security levels for different network devices according to the security risk level and grant different permissions.

3. Dynamic authentication: Use different authentication methods while ensuring the dynamic nature of authentication, and encrypt the authentication password to enhance the security of user login.

4. Data backup: Using two servers to perform mutual data backup for the network information system to prevent data loss and establish a connection between the two servers. In the event of an abnormal situation on one server, the other server can promptly and effectively backup the data of the abnormal server and issue an alert notification.

5. Authorization setting: The network information system sets up authorization for access between different areas. The network management department assigns different authorization levels to different objects with different security risk levels without the need for separate settings, which is convenient.

6. Security log: The operation records, security risk detection, virus invasion, vulnerability checks and other aspects of the network information system are saved in the form of a security log, providing reference for the corresponding operation and maintenance.

## 6 Discussion

Updating or revising regulations and standards is a good practice because the field of network security is constantly evolving and changing. New technologies and methods may emerge that impact security frameworks and models. These changes may render existing regulations and standards ineffective or inapplicable. For example, new attack methods may render previous security measures ineffective. Therefore, continuously updating

regulations and standards ensures that security frameworks and models are able to effectively protect networks from attacks.

Additionally, as the network environment changes, so do network usage patterns. This may cause existing regulations and standards to become inapplicable. For example, as more people use cloud services, network security risks also change. Therefore, updating regulations and standards ensures that security frameworks and models can adapt to new network environments.

Furthermore, updating regulations and standards also helps organizations better protect their networks and data. When organizations follow the latest regulations and standards, they can better understand the latest in network security knowledge and ensure that security measures are effectively preventing attacks and protecting data.

Overall, updating or revising regulations and standards is an important practice in network security because it helps organizations adapt to new technologies and network environments, protect networks and data from attacks, and meet regulatory requirements.

## 7 Conclusion

After conducting research on relevant literature on security frameworks and models, a security framework was designed for CoffeeBlend company with the aim of protecting its network security. The security framework will provide multiple features including security level configuration, data backup, dynamic user authentication and permissions management, and security logs. It is believed that these features will assist in protecting CoffeeBlend company's network from attacks and help the company respond to network security threats.

## 8 Reference

- [1] Muhamet Gërvalla, Naim Preniqi, Peter Kopacek, "IT Infrastructure Library (ITIL) framework approach to IT Governance," IFAC-PapersOnLine, vol. 51, no. 30, pp. 181-185, 2018.
- [2] A. Santos Olmo Parra, L. E. Sanchez Crespo, E. Alvarez, M. Huerta and E. Fernandez Medina Paton, "Methodology for Dynamic Analysis and Risk Management on ISO27001," in IEEE Latin America Transactions, vol. 14, no. 6, pp. 2897-2911, June 2016.
- [3] K. Thakur, M. Qiu, K. Gai and M. L. Ali, "An Investigation on Cyber Security Threats and Security Models," 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015, pp. 307-311.
- [4] D. B. Rawat, R. Doku and M. Garuba, "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security," in IEEE Transactions on Services Computing, vol. 14, no. 6, pp. 2055-2072, 1 Nov.-Dec. 2021.
- [5] B. Schneier, "University Networks and Data Security," in IEEE Security Privacy, vol. 4, no. 5, pp. 88-88, Sept.-Oct. 2006.