

Assignment

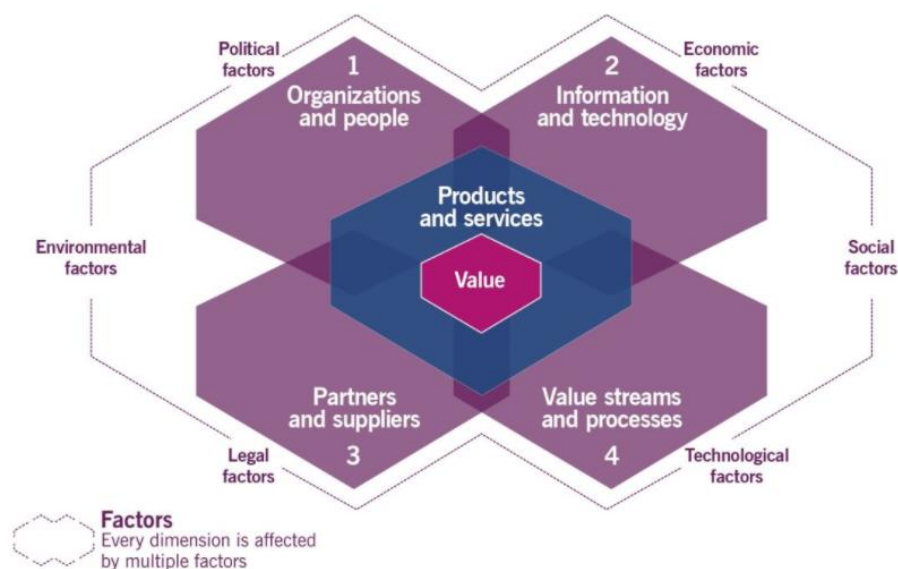
1. security framework or models

1.1 Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library (ITIL) is a collection of methods and practices useful for managing the development and operation of information technology infrastructures. The ITIL has been produced as a series of books, each of which covers an IT management topic. Since it includes a detailed description of a many significant IT-related practices, it can be tailored to many IT organizations[1].

ITIL, as the best practical knowledge system in the global IT service management field, has provided guidance for IT managers through publishing, training and certification in the past 30 years, especially those engaged in operation and maintenance. The latest version ITIL4 provides a flexible and coordinated SVS system, which adapts all organizations. By helping the organization to adjust human, digital and physical resources, the organization can compete in modern complex environments, support the organization adjusted to the new environment. At the same time, we have also absorbed a lot of content about customer experience and value chain, making our delivery and management more streamlined, practical, and maximizing service value. In order to meet the agile requirements facing digital transformation, it also combines many new theories and methods, such as lean, agility and devops. The ITIL4 frame contains two core contents: service value system (SVS) and service. The most important value of the SVS system is "eliminating the island of organization". From the basic level, itil4 emphasizes the importance of collaboration, transparency, as much as possible, and overall work. ITIL has delivered end -to -end value delivery from providing services. The focus is now to create value through service relationships. The value of the four dimensions is reflected in the service management of the digital age to fully think based on the four perspectives, which can not only achieve the high quality and efficiency of management, but also increase the success rate of service and project management at the same time.

The goal of ITIL is for organizations to create predictable IT environments and to deliver the best customer service possible to customers and clients by streamlining processes and identifying opportunities to improve efficiency. ITIL has always focused on integrating IT into the business — something that has become increasingly important as technology becomes a vital aspect of every business unit. ITIL 4, the latest iteration of the ITIL framework, maintains the original focus with a stronger emphasis on fostering an agile and flexible IT department[2].



ITIL 4 contains seven guiding principles that were adopted from the most recent ITIL Practitioner Exam, which covers organizational change management, communication, and measurement and metrics. These principles include:

- Focus on value
- Start where you are
- Progress iteratively with feedback
- Collaborate and promote visibility
- Think and work holistically
- Keep it simple and practical
- Optimize and automate

1.2 ISO 27000

(1) ISO27000 Information Security Management System Overview

Information Security Management System (ISMS) is a series of management activities such as risk assessment establishment, implementation, operation, surveillance, review, and continuous improvement of information security based on the overall management activities of the organization. The system of organizations and goals in the overall or specific scope, and the method of achieving the methods used in these goals.

ISO/IEC27001 is a standard for establishing and maintaining the information security management system.

(2) ISO27000 information security management system certification benefits

Organization can refer to the information security management model, and establish a complete information security management system in accordance with the advanced information security management standard ISO 27001 standards, and implement and maintain it. The information security management method uses the lowest cost to reduce the probability and result of information risk to acceptable levels, and take measures to ensure that the business will not be interrupted due to the occurrence of risks. Organize the establishment, implementation, and maintaining information security management system will be:

- Strengthen employees' information security awareness, standardize organizational information security behavior;
- Comprehensive and systematic protection of the organization's key information assets to maintain competitive advantages;
- When the information system is attacked, ensure that the business continues to carry out and minimize the loss;
- Make the organization's business partners and customers confident in the organization
- Enhance the market competitiveness of the enterprise by complying with international standards and enhance corporate image

(3) ISO27000 information security management system certification process

Research and Planning of the Status of Management System -Standards and Document Writing Training -System Document Establishment -System Operation -Internal Management System Review -Management Review

1.3 Information Security Governance Framework and Models

The Information Security Governance Framework is a managerial model that provides guidance in the development and implementation of an organizational information security governance structure.

The core of the Information Security Governance Framework includes recommendations for the responsibilities of members of an organization including: Board of directors/trust Senior executives. Executive team members who report to a Senior managers. All employees and users[3].

1.3.1 Security architecture models

Security architecture models illustrate information security implementations and can help organizations to quickly make improvements through adaptation. Some models are implemented into computer hardware and software, some are implemented as policies and practices, and some are implemented in both. Some models focus on the confidentiality of information, while other focus on the integrity of the information as it is being processed.

1.3.2 Access Control Models

Access controls regulate the admission of users into trusted areas of the organization—both the logical access to the information systems, or the physical access to the organization's facilities. Access control is maintained by means of a collection of policies, programs to carry out those policies, and technologies that enforce policies.

2. Some aspects that organizers should focus on.

2.1 Overall aim

By increasing the construction database audit, database access control (database firewall), encryption, operation and maintenance departure, and data security trend, supplement data security shortcomings, and optimize and upgrade existing data asset management, desensitization, and interface security (Consider increasing the number of databases and improvement performance) to meet the needs of employee information and product information security. Finally, the overall situation of structural data protection is achieved through process, and CofeeBlend will be assisted in forming a comprehensive data security protection system.

2.2 Implementation plan

Taking the new data security situation as a comprehensive management and control platform for data security, classify 7 data security issues given as data asset management, desensitization, interface security management, encryption, and database audit, database firewalls, operation, and maintenance. Starting from the perspective of possibilities and applications, achieve the ability to deal with structural data security issues

2.3 Data asset identification management

Achieve automated data classification and dynamic data asset analysis through active scanning methods, database protocol analysis, high-efficiency data recognition and visualization technologies. Provide data assets visualization, management and tracking, and strong data interface support to support the multi-channel and multi-scenario application with the internal data.

2.4 Data desensitization management

Provide a variety of desensitization schemes to ensure that the data can still retain the original semantic and associated relationship after desensitization, at the mean time ensuring the availability, normality and authenticity of the data in each scenario.

Provide the protection of privacy data, improve the quality of test data, and reduce the burden on staff.

2.5 Interface security management

Provide standard foreign cooperation plans, and evaluate the interface usage according to the results of data filing of foreign cooperation. Provide data interface audit functions, ensure data security compliance while enhancing comprehensive security detection capabilities. Provide comprehensive data inspection methods, develop sharing detection and the interface sensitive information detection to the outside world. Achieve the combination of upstream and downstream of the security chain.

2.6 Encryption

Sensitive data is stored in the form of a ciphertext to ensure that the sensitive data is safe even if the storage medium is stolen or the data file is illegally copied. Through the separation of the three aspects through password technology, avoid the risk of batch data leakage caused by password leakage. The encryption system has excellent security and processing capabilities, and can be transparent in the system without modifying the original application.

2.7 Database audit

Database security products based on database communication protocols and SQL analysis technologies can monitor records of all access behaviors of the database in real time, and alert the risk behavior suffered by the database to help users quickly trace the cause of the accident.

Visual database asset visits and risks, trace on security incidents, and carry out the incidents, tracking, accountability, and determining responsibilities. Illegal access data such as risk access and SQL attacks should be alarmed in time.

2.8 Firewall of the database

Active defense mechanism based on behavioral analysis can actively monitor, identify, alert, and block the security threats for databases, and realize the behavioral analysis, access behavior monitoring and hazardous operation blocking of the database. Fundamentally solve the various data security issues faced in the data operation process, effectively meet the requirements of internal security needs and the requirements of external national compliance security management specifications. Prevent external attacks, data stolen, prevent internal personnel from leaking, and prevent sensitive data from being unauthorized access.

2.9 Database operation and maintenance

The database security operation and maintenance system intercepts and modify the database communication content, and processes the sensitive data in the database online shielding, character replacement, random replacement, etc., and controls the access permissions of sensitive data. For sensitive data stored in the database, users with different authorities will be displayed by different results through desensitization systems. Control users' access to sensitive data, and reduce data leakage during online access and operation and maintenance.

2.10 Compliance (Laws and Ethics)

The main difference between legal compliance and ethical responsibility is that the legal compliance is bound to obey whereas the ethical responsibility is a choice. Security of personal staff's data, client's data and company's intellectual properties should be treated as the same level. Privacy is the most important thing that should never be sold out.

2.11 Contingencies Planning

According to the Hartford insurance company, over 40% of businesses that don't have a disaster plan go out of business after a major loss. So having contingencies planning is really important.

2.12 Data internal leakage prevention

- (1) Access permissions of business system operators and R & D personnel shall be controlled, establish corresponding roles and allocate access permissions according to the principle of demand, and assign specialists to audit the access to the business system.
- (2) Establish a terminal access mechanism and uniformly deploy anti -virus and terminal control software.
- (3) Through safety awareness training, cultivate good terminal use habits to avoid data from being stolen through the terminal.
- (4) Before the internal application system is officially delivered, a comprehensive software test should be done to avoid hidden data call interfaces. And do a good job of penetration testing before the official launch to avoid attackers to obtain data in batches through vulnerabilities such as data traversal, unauthorized access, and SQL injection.

2.13 Summary

In all,in this chapter I suggest coffeeBend to focus on these aspects.

- (1) Data asset identification management
- (2) Data desensitization management
- (3) Interface security management
- (4) Encryption of important assets.
- (5) Database audit
- (6) Firewall of the database
- (7) Database operation and maintenance
- (8) Contingencies Planning
- (9) Data internal leakage prevention

3.my approach to meet the need of the company's data security

3.1 Company profile

Jamaica's blue Mountain Peak coffee is one of the greatest and most sought-after mixes in the world, and CoffeeBlend sells it. CoffeeBlend has a large presence all over the world.

3.1.1 Demand analysis

Because of its big workforce and foreign client base, the firm has recently been under intense pressure to allow both employees and customers to access the company's network/resources using their own devices. The company's main priority is the security of personal personnel and client data. The corporation is also concerned about safeguarding its billion-dollar intellectual property. As a result, the following issues arise in the given implementation:

- Protect its intellectual properties
- A large amount of user information will not be stolen
- Stably provide services to employees/households
- Provide more automated cloud services
- The company has insufficient IT operation and maintenance training

3.1.2 Scope

Based on the above requirements, I formulated a specific transformation plan. The whole plan consists of three parts. The first part is based on the ITIL theoretical framework to implement the standardization, and process of the operation and maintenance system; the second part is based on the DevOps theory to greatly improve the operation and maintenance the level of automation; the third part is to strengthen communication between the operation and maintenance team.

3.2 Governance and Strategic Planning for Security

The standardization of the operation and maintenance system means that every routine operation and maintenance work has relevant document guidelines. These routine tasks cover server shelves, on-duty inspections, daily backups, emergency handling, etc. All operation and maintenance personnel perform operation and maintenance work following the document guidelines, rather than relying on their technology to fight on their own. It is necessary to fully integrate ITIL's ideas and rely on the construction of an integrated ITIL system to implement the standardization, standardization, and process of the operation and maintenance system.

3.2.1 Building an integrated ITIL system

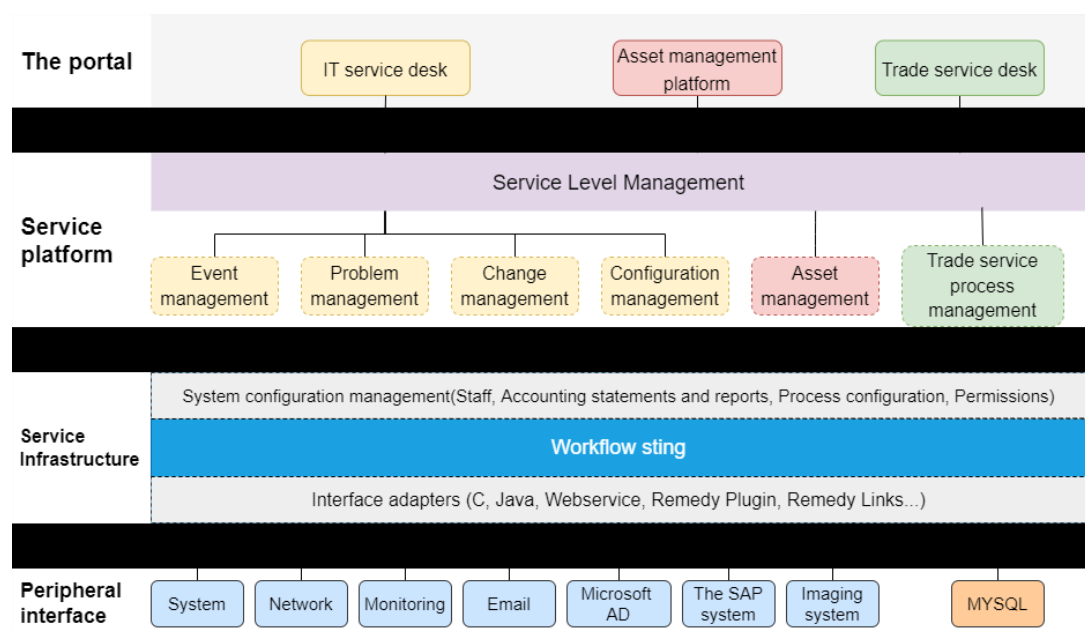
The ITIL system design needs to meet the following functions[4]:

- (1) It needs to include the main modules of ITIL: change management, incident management, problem management, data maintenance, configuration management, service request, service level management, authority management, etc. It also needs to include personal salary and support the display of charts, such as pie charts, bar charts, etc
- (2) Provide a third-party API interface, which can be connected to CoffeeBlend's existing OA system, program publishing platform, test platform, mobile office system, and other systems. Approval of changes and other processes can be carried out through the mobile terminal.
- (3) The configuration management module needs to realize an automatic collection of system configuration information, rather than manual entry, to ensure that the configuration information is complete and accurate.
- (4) The system needs to support secondary development, customer-defined modules, easy to transform and upgrade, select mature software developers, and have

many successful cases in the catering industry. The interface is friendly, using the WEB interface, there are few entries, and the information is brought in from the configuration library.

3.2.2 Optimize ITIL operation and maintenance management process

The scope of this project is mainly composed of three sub-projects, which are the IT service desk, transaction service desk, and IT asset management. Among them, the transaction service desk is a solution for customers to order online orders and employees to find orders online. With the transaction service center as a pilot, a service desk model of the business operation unit was established to provide platform-level support for the efficient operation of business operations. The logical framework diagram of the overall solution is as follows:



3.2.3 Configuration Management Automation

The new ITIL platform configuration management module plans to use agents to automatically collect basic information such as servers, databases, and applications,

which solves the problem of inaccurate configuration information and large manual input by operation and maintenance personnel. It is planned to establish a configuration management team, promote the implementation of configuration management naming and configuration management specification documents, and sort out the existing system names, forms, and levels of configuration management. Promote the docking of the quality control platform, project management platform, and cloud management platform with the new ITIL platform configuration management module. Automatically collect network equipment information, improve architecture diagram display technology, and register application configuration attributes, and generate upstream and downstream relationship topology diagrams through network collection. Continue to advance through the configuration management data operation report, and urge the responsible person to maintain and confirm the configuration management information promptly in the form of tasks.

3.3 Improve the automation level of operation and maintenance

Due to the low level of operation and maintenance automation, the satisfaction of processing and fulfilling IT requirements are low. As the system service The increase in servers has also led to increased pressure on operation and maintenance engineers. Manual operation alone cannot meet the increasing demands of business departments. Increasing IT system requirements need to refer to the DevOps operation and maintenance model to greatly improve the automation level of operation and maintenance.

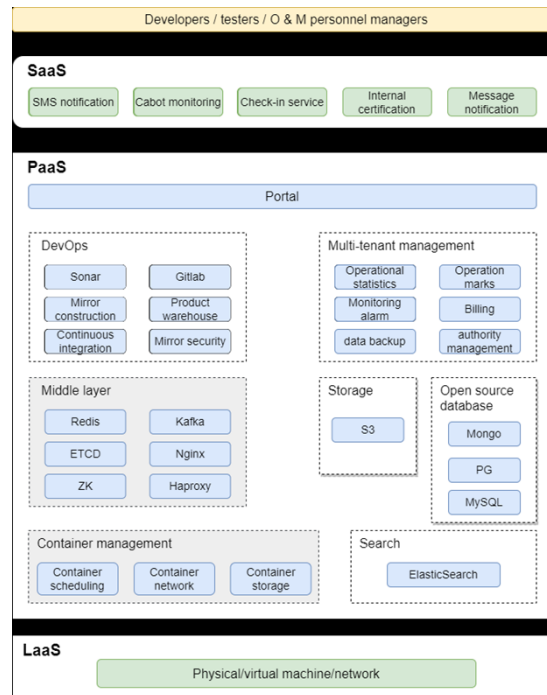
(1) Realize the DevOps operation and maintenance model[6]

Establish a culture of communication and cooperation between development and operation and maintenance teams, resolve existing conflicts between development and operation and maintenance teams, bridge the gap between them, and promote more communication, cooperation, and trust. At the same time optimize the existing KPI

performance appraisal, establish OKR (Objectives and Key Results), set the common goal of the two teams, and be output-oriented, and the output of the IT department is to empower the business, let the system go online as soon as possible, and run stably, based on this, refine the corresponding target performance orientation, so that the two teams have a sense of honor and responsibility.

(2) Building a cloud computing platform

The rapid development of CoffeeBlend is inseparable from the rapid construction of IT systems, and the rapid construction of IT systems is based on IT infrastructure. IT infrastructure resources include networks, servers, storage, databases, middleware, etc. Cloud computing has been developed for more than 10 years and is now a very mature technology. Cloud computing is a distributed computing technology that integrates network, server, storage, and other resources through software technology to realize computing resource sharing and on-demand Allocation, users can apply for resources on the "cloud" at any time, use them according to their needs, and pay for usage to maximize the use of resources, reduce usage costs, and improve the automation level of operation and maintenance. CoffeeBlend IT operation and maintenance center plans to realize the rapid delivery of IT resources by building a cloud platform, and building a unified standard IaaS, PaaS, and SaaS cloud platform, as shown in Figure 5-6. The IaaS platform will integrate physical machines, virtual machines, and network resources; the PaaS platform includes DevOps platforms, multi-tenant management, middleware, storage, open-source databases, container management, and search. The DevOps platform includes DevOps components such as Gitlab, mirroring construction, and product warehouses, which are used to implement a part of DevOps functions. Multi-tenant management includes functions such as operation statistics, operation traces, monitoring alarms, billing bills, data backup, and authority management.



3.4 Improve service level

Conduct ITIL, DevOps, and AIOps training. Through ITIL, DevOps, and AIOps training and promotion, employees' awareness of operation and maintenance processes and knowledge of operation and maintenance management are improved, so that employees understand that only by improving operation and maintenance efficiency can they release productivity, automate routine and repetitive tasks, and reduce human errors. Reduce the pressure of operation and maintenance, so that operation and maintenance personnel can have more energy to learn more skills, do more valuable things, and improve personal capabilities.

3.5 Contingencies Planning

To restore the business as quickly as possible, it is necessary to minimize the duration of detection, diagnosis, and repair to minimize the impact on users and businesses. To ensure the efficiency of each link in the event process, operation and maintenance personnel need to follow the following principles:

- (1) Anything must be reported: An incident work order is established as soon as an incident occurs, and the incident process is followed in an orderly manner.
- (2) Quick response: Take the restoration of the IT service level as the primary goal, and quickly respond to incident handling. For emergencies and major incidents, under the premise of ensuring efficient communication, it is not necessary to fill in a work order, and make a supplementary record after the incident is handled.
- (3) Emergency first: When multiple events occur during the same period, resources should be allocated to high-level events first according to the event level, and they should be handled level by level according to the level of the event and the causal relationship.
- (4) Full follow-up: After the incident, the front-line post is responsible for tracking the incident until the business service is restored and the work order is closed.
- (5) Accurate records: Accurately record incident reports, diagnosis, and analysis, disposal recovery, verification and closure, etc., and regularly report or notify relevant parties following clear rules.

3.6. Summary

List the improvement measures for CoffeeBlue's problems, and then classify these improvement measures to organize a specific optimization plan: (1) Based on ITIL theoretical framework, optimize the change management, fault management, and other processes, implement the standardization of the operation and maintenance system, standardization and proceduralization; (2) Based on DevOps theory, vigorously improve the automation level of IT operation and maintenance; (3) Strengthen the communication of the operation and maintenance team. At the same time, the above three solutions are detailed and discussed, and it is pointed out that the process of implementing the standardization, standardization, and process of the operation and

maintenance system must first build an integrated ITIL system; it also points out that through the promotion of the DevOps operation and maintenance model and the construction of a cloud computing platform, Improve the automation level of operation and maintenance; specific measures are given to strengthen the communication of the operation and maintenance team.

Reference

- [1] <https://en.wikipedia.org/wiki/ITIL>
- [2] <https://www.servicenow.com/uk/products/itsm/what-is-til.html>
- [3] <https://moodle.uwtsd.ac.uk/course/view.php?id=2809>
- [4] <https://www.zhihu.com/search?type=content&q>
- [5] Teresa Lucio-Nieto,Dora Luz González-Bañales. Exploring ITIL® Implementation Challenges inLatin American Companies[J]. International Journal of Information Technologies and SystemsApproach (IJITSA), 2019(1):73-86.
- [6] Li Xiang. Research on Optimization of IT Operation and Maintenance Management of PC Insurance Companies Based on ITIL Method[D].East China Jiaotong University, 2020.

