

Assignment

Name: Bowen Chen
Student ID: 2200373
Course: Data Security

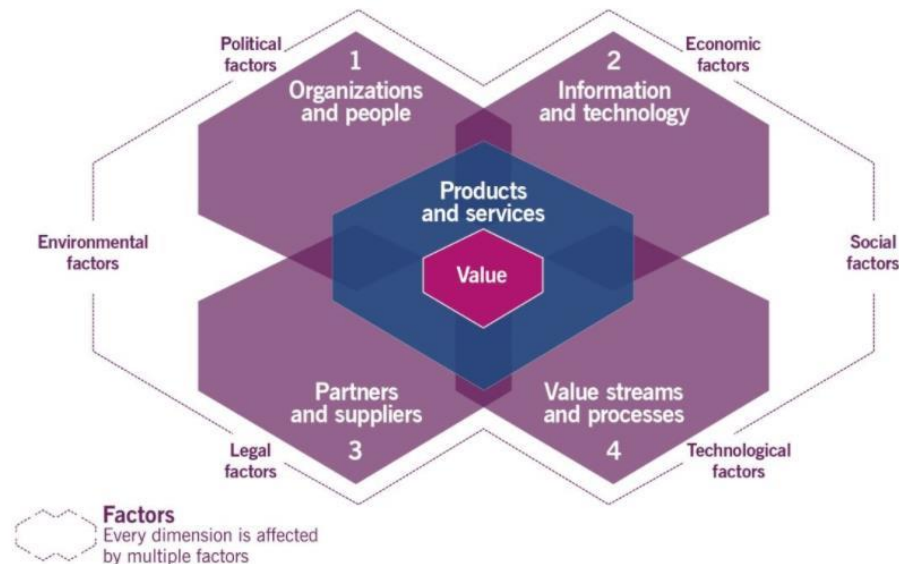
1. security framework or models

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.



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

1.3.1 Data security capacity maturity model ---- DSMM

It stipulates the requirements of data collection security, data transmission security, data storage security, data processing security, data exchange security, data destruction security, and general security maturity level requirements.

The DSMM architecture consists of the following three dimensions:

(1) Safety capacity dimension: The security capacity dimension clarifies the capabilities that organizations should have in the field of data security, including organizational construction, institutional processes, technical tools and personnel capabilities.

(2) Mature level dimension: The maturity level of data security capacity is divided into level 5, which specifically includes: level 1 informal execution level, level 2 plan tracking level, level 3 full definition level, level 4 quantitative control level, and level 5 continuous optimization level.

(3) Data security process dimension:① The data security process includes data survival cycle security process and general security process.② The safety process of data survival cycle includes: data collection security, data transmission security, data storage security, data processing security, data exchange security, data exchange security, data destroyed security.

1.3.2 PDR Model

Protection-detection-response (Protection-Detection-Response, PDR) model is a model commonly used in information security guarantee. It is the earliest network security model that reflects active defense ideas. The threat facing the information system ensures the security of the system by adopting moderate protection, strengthening testing, implementing response to security events, and establishing protection of threats.

1.3.3 CMMI DEV V2.0 Model

In order to cope with the challenges of continuous changes in the global business pattern, CMMI DEV V2.0 will help enterprises establish and improve key capabilities through benchmark comparison to improve corporate performance. It is a verified global best practice. It aims to

optimize the business performance in the changing global environment, help organizations to establish the key capabilities to solve the most common business challenges and set the corresponding benchmark, including: (1) design and development of products

- (2) Improve performance
- (3) Delivery and management services
- (4) Maintain habitual and persistent
- (5) Management business elasticity
- (6) Planning and management work
- (7) Choose and manage suppliers
- (8) quality assurance
- (9) Managed employee
- (10) Support implementation

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

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.

Sensitive data owned by enterprises, including business secrets, intellectual property, key business information, business partner information or user information. The personal information involved in personal privacy is the most important and wide sensitive information in the information system.

Personal information: Refers to various information that can be recorded alone or with other information to identify the personal identity of natural persons alone, including but not limited to the name of natural persons, date of birth, ID number, personal biometric information, address, telephone number Numbers, etc.

Personal information of citizen: refers to a variety of information that can be recorded alone or with other information to identify specific natural persons or reflects the activity of specific natural persons, including name, ID number, communication and communication contact information, address, account number, account number, address, account number Password, property status, trajectory, etc.

Personal suggestions: For sensitive data, technical measures are used to limit access and use of user information.

- 1) Confirm that you need to view the background account of the customer's personal information, the account authority is the permissions of the business;
- 2) Query customer personal information can only query the information after desensitization as much as possible. For example, the phone number and ID number only retain 4 digits before and after, and the intermediate content is desensitized;
- 3) Do not do it at the front end whether requesting verification or desensitization. The front end is unreliable;
- 4) For back -end accounts that need to export customer personal information, confirm whether it is necessary to export the customer's personal information,
 - a) If there is no need to recommend the export of the customer's explicit information;
 - b) If the clear text information of the customer's personal information is indeed necessary, it is recommended to strictly limit the scope of the user of the background account (user, the source IP login), and set the exported information range, such as information numbers and information

duration , all the inquiries and exports of customer information are recorded.

The principle and function of the data desensitization system of desensitization implementation[4]:

Step 1: Evaluate the security level of data assets, and formulate different desensitization strategies according to different security levels and data requirements.

Step 2: Set off desensitization tasks and trigger conditions, and call conditions such as time and data processing process.

Step 3: After triggering desensitization conditions, the desensitization system will send the execution algorithm package of the desensitization algorithm to send each node to achieve data desensitization.

Data desensitization can occur in two stages:

- 1) Data collection phase to achieve the most basic and simple desensitization;
- 2) During the application of data assets, real -time desensitization is performed for different applications, and the application desensitization is relatively complicated and variable.

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.

Interface call monitoring: limit the number of access times, maximum connection, real-time monitoring of interface traffic, abnormal traffic alarm, such as SMS interface, withdrawal interface, recharge interface, etc.

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. Using 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.

The data preserved and transmitted data provides a encryption function, and the data security protection is provided on the two dimensions:

1. Confidentiality: Use encryption to ensure that only users who have the corresponding key can access the protected data;
2. Integration: ensure that information is not viewed and modified during the storage and transmission process, such as: transmission with SSL, and using encryption algorithm + dynamic token verification for sensitive information (such as username, password, and important ID value).

When the encryption algorithm, random number use, and encryption protocol, you need to take into account performance considerations. You need to distinguish the data, and only encrypted data that needs to be encrypted.

The encryption technology is based on the security of the key. If the key is leaked, it will lose security. In actual development, the key is written directly in the source code, or in the configuration file, the online

and the development environment configure the same keys. In this case, it is not safe enough.

Improve through two solutions:

1. The keys and algorithms are placed on an independent server, and even make a dedicated hardware device to provide encryption and decryption services outside the outside world. Use the program to call this service to achieve data decryption. This method is maintained by a special person. The key is not easy to leak, but the cost is higher.

2. Place the additional solution algorithm in the application system, and the key is placed in an independent server. In order to improve the security of the key, when the actual storage, the key is cut into several pieces. After encryption, it is stored in different storage media at the same time as the security of the key, it also improves performance.

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[5].

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. The operation and maintenance monitoring of the operating and maintenance management system, the use of resources such as CPU, hard disk, memory, network and other resources of the server, as well as system service levels to detect and alert.

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[4].

1) Classification of disaster recovery:

Data -level disaster recovery: Create a different place data system, which is a available replication of local key application data. When a disaster occurs in local data and the entire application system, at least there is a key business data in different places. This data can be completely replicated with the local production data, or it can be slightly behind the local data, but it must be available.

Application -level disaster recovery: On the basis of data -level disaster recovery, establish a set of backup environments that are equivalent to local production systems in different places, including hosting, network, application, IP and other resources. Can provide a completely available production environment.

(2) Backup strategy

The backup strategy is the core part of the backup solution. Different backup strategies should be developed in accordance with the importance of data and data management. The backup strategy includes: backup object, backup method, backup frequency, preservation time limit, etc. For example, the data pump is backup twice a day, RMAN is back up once, and the backup is stored in double portions.

2.12 security audit

Try to deploy the log audit system to monitor various operations and attack information in real time. According to the rules of the settings, intelligent judgments have been determined by various risks, and the police are alarm.

The classification of logs includes: application system logs, operating system logs, database logs, network equipment logs and information security equipment logs. The following basic content should be recorded in each type of log: the date, time, and event description of the incident, the

operator information, the introduction, export, success and failure operation. When customers visit the portal, they should record and save the login behavior, business operation and system operation status to ensure that the operation process can be traced and audited. And ensure the security of business log data. The log record should meet the following security requirements:

Record key business operation logs: the logs of key business operations should be recorded, such as login success and failure, key business processing, sensitive data query, sensitive data import and export.

Record the application system running log: the start -stop, abnormalities, and resource usage of the application system should be recorded.

Sensitive data blur: prohibit sensitive information such as service passwords in business logs. If you really need to record sensitive information, fuzzy processing should be performed.

To prevent business logs from deception: If you need to introduce data from non -faithful sources when generating business logs, you should be strictly verified to prevent cheating attacks[5].

Business log security storage and access: It is forbidden to save business logs in the web directory to ensure the secure storage of business log data and strictly restrict access to the access of business log data. Copy the signature of the business log records to achieve tampering. The log record should be stored online for at least half a year, and it is stored offline for 1 year[6].

2.13 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.

2.14 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

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.