Enterprise Information Infrastructure Constructed by Integral Planning

Shyh-Chang Liu, Tsang-Hung Wu
I-Shou University, Kaohsiung, Taiwan, Republic of China

Abstract

Following the progress of technology in recent years, enterprise is paying more and more attention to the issue of information security. Although enterprise spends lots of resources, the customers are not satisfied even complained. The main reason is information technology lacks of enterprise integral planning. This paper will first discuss on ITIL, ISO27001 risk management and commonly seen information protection technology, and how to establish the enterprise information.

1. Introduction

Following the development of information based, information system plays a more important role in enterprise day by day. In addition, in order to enhance competitive strength and to combine information technology with commercial activity successfully, consideration has to be given on the start out from the view angle of enterprise operation. In order to survive and to maintain daily operation, enterprise has to establish various kinds of different commercial flows to complete its operation objectives both in short-stage and long-term. Furthermore, requirement for information technology increases day by day. Therefore, the ratio occupied by investment in information infrastructure becomes more and more. It is difficult to materialize the performance data of information technology. Most often top management and other department users are under the impression that enterprise put in a lot of cost on information technology, but this cannot provide the proof that it can bring profit to the enterprise. As a result, the information technology department in the enterprise always categorized as a money spending unit. Moreover in the management activity of daily information service, as there is lack of good communication channel and method between users, even if the information technology department put in a lot of time and manpower to solve problems of users, yet this cannot reach the requirement of users. As a result, what is obtained is complaint on the information technology department by other department users. Consequently, there exists contradiction between the positions of the information technology department and other department. How to make use of limited manpower to manage the continuous increase of anticipation of users and to continue to reduce the budget of the information technology department is the challenge met by the information technology department at present. Currently the information security of a great majority of enterprise still relies on security technology but no appropriate management rules for its implementation. Information security of enterprise may be damaged through many ways such as unauthorized utilization, computer virus ...etc. The scope of effect due to the damage on information security may be beyond expectation. Loss of sensitive or key business information not only will directly affect the competitive strength of enterprise, but also will result in negative effect on its image. Therefore consideration should be given to the establishment of a comprehensive information security system so as to conform to the three principles of information security including Confidentiality, Integrity and Availability. The meaning of confidentiality is to provide guarantee that the necessary control on every information processing can be enhanced and the stealing of unauthorized information can be prevented. The meaning of integrity is to judge whether the original appearance of the content of the information can be maintained and is not altered. The meaning of availability is to be able to prevent the collapse of service and work ability. The Figure 1 explains that the protection on enterprise information and asset requires formation of combination of layers upon layer of protection system. This paper will first introduce the method of information technology flow service management ITIL and the international standard of risk management ISO27001. Then it will explain frequently seen information attack method and protection technology. Finally, this paper will provide suggestions on the direction of establishment for enterprise in order to improve the information operation flow of enterprise.

Figure 1. Enterprise multiple protection system
2. The essence of ITIL/ISO27001

Information Technology Infrastructure Library (ITIL) is a service management standard architecture developed by the Central Computer and Telecommunications Agency (CCTA) in the mid-90s aiming at the information domain. ITIL [1, 2, 3, 4] presents eleven management flows and hereunder are explanations on various flows:

(a) Services Level Management (SLM): according to customer requirement it is applied to manage the type and quality of the required information service being provided, to sign agreement and to execute effectively according to the agreement.

(b) Financial Management for IT Services: its purpose is to provide various cost information generated during the processes of provision of information service, for example: providing information of different price calculation method. It is helpful that the relationship between cost and benefit can be sufficiently considered during selection of certain information infrastructure or information service.

(c) Capacity Management: in order to ensure that the service level signed with customer can be achieved; analysis and planning on procurement time and subordinate resource are conducted through the present and future capacity and efficiency requirement.

(d) Availability Management: availability management is the deployment through appropriate resource, method and technology so that the provision of normal service can be ensured. It mainly involves in the optimal planning of the maintenance activity and design of relevant measures in order to reduce the number of occurred incidents to a minimum. In this item, this may include coordination and contract with companies outside to conduct system maintenance work in order to enhance the availability of service.

(e) IT Service Continuity Management: IT service continuity management is the planning and coordinating flow on relevant technology, finance and resource management conducted after the occurrence of a disaster in order to ensure that the continuity service agreed with customer can be maintained and to avoid interruption on the business operation.

(f) Service Desk: this is the liaison channel for users and the information technology department when the problem happened on the utilization of service. On the response time on one problem, this will be stipulated in the Service Level Agreement (SLA) after the communication between users and the information technology department. In addition, the information technology department is required to provide statistical information to the SLM in order to confirm whether the SLA can be reached.

(g) Incident Management: the primary goal of incident management is to solve incident and to restore the supply of service as soon as possible. In such a way, it can guarantee that the service standard can be maintained continuously.

(h) Problem Management: if there is doubt that a problem existed in the information infrastructure, then the objective of the problem management is to find out the possible reason for generating such problem. Once the reason for generating the problem is found out, then relevant contingency measure should be stipulated. Such problem is categorized as Known Error and it is required from business decision whether one time permanent correction is needed in order to prevent reoccurrence of similar incident.

(i) Configuration Management: This flow mainly conducts control (standardized and status monitor) aiming at the information infrastructure that continues to change. All important components in the infrastructure will be identified first and the information of these components will be collected, recorded and managed. Finally this information will be provided to other flows, and the storage database is called Configuration Management Database (CMDB).

(j) Change Management: this flow is to conduct examination and control during the implementation of changes on the information infrastructure and these changes are carried out under the condition of generation of minimum negative effect. In addition, the process of the change will only commence under the monitor of configuration management status and coordination of change request originator, problem management and many other flows.

(k) Release Management: release refers to the deployment after test and guide in of a set of configuration items of actual operation environment. Mainly this is to ensure the success of the first time guide in of the actual operation environment on-line including integration, test and storage. Moreover, it is also required to ensure only correct software version after test and authorization and hardware can be supplied to information infrastructure. The same set of multiple versions software will be imposed software control through a Definitive Software Library (DSL).

2.1. The substance of ISO27001

The forerunner of ISO 27001 [5, 6, 7] information security is BS7799 that is an international information security audit standard. It was presented and amended by the United Kingdom Standard Association in 1995 and was included by the International Organization for Standardization (ISO) as the international standard. BS7799 is mainly divided into BS7799-1 and BS7799-2. ISO17799: 2005 (BS7799-1) is utilized mainly as a reference document that provides broad security control measure as the best operation method for the present
information security. It includes 11 domains, 39 control items and 133 control essentials. However, these are not utilized as the standard for appraisal and certification. BS7799-2 : 2005 was revised as ISO27001: 2005 information security management system international standard in 2005. It establishes the concrete requirement for implementation and in written form. According to the needs of the organization, the requirements for the implementation of security control measures are specified and at the same time it is utilized as the standard for certification and appraisal.

ISO 27001 is the ISMS standard that abides by the Plan-Do-Check-Model (PDCA) to conduct continuous and effective risk control as in Figure 2[8]. The so-called Information Security Management System is part of the overall management system that is stipulated according to the enterprise risk management method. It is utilized to establish, execute, operate, monitor, examine, review, maintain and improve the information security in order to achieve the most appropriate information security risk control.

There are four main parts illustrated here:
(a) Plan: establishes the information security management system, the information security policy and management risk and improves the policy, objective, process and procedure of relevant ISMS of the information security in order to generate uniform results for the overall policy and objective of the organization.
(b) Do: actually does and executes the policy, control measures, process and procedure of the ISMS.
(c) Check: appraises according to the policy, objectives and actual experience of the ISMS, measures the processing performance during trial use and reports the result to the management for examination.
(d) Action: adopts rectification and preventive measures according to the internal audit and management level audit result on the security management system in order to achieve continual improvement on the ISMS.

ISO27001 control items include:
(a) Information security policy: provides management guidance and support principle for information security.
(b) Information security organizational: manages the information security in the organization, maintains the security of the information processing facilities and provides to third party during access of information asset; maintains information security when the information processing is outsourced to other organization.
(c) Asset classification and control: conducts categorization on the information asset of the enterprise and adopts appropriate protective measures.
(d) Personnel security: reduces the risks of human error, theft, fraud or misuse of facility. Ensures that users can understand the threats and problems of information security and has the ability to support the security policy of the organization in the daily work. Diminishes the damage caused by security and non-effective incident to a minimum and supervises learning from this type of accident.
(e) Physical and environmental security: avoids access, damage and interruption on the operation site and information. It evades the loss, destruction or damage of assets as well as the operation activity interrupts; keeps away from the jeopardy on the information processing facility or the stealing of information.
(f) Communications and operations management: ensures correct and safe operation of information processing facility, reduces system failure risk, and protects software and information integrity to be free from damage by malicious software. It also maintains the integrity and availability of information processing and communication service. That ensures information security inside the network and protects the supported infrastructure, avoids damage on asset and interruption on enterprise activity, and evades loss, alteration or misuse of information during exchange between organizations.
(g) Access control: the object is to manage the access behaviors of management information and to guarantee that the access authority’s limit of the information system can be adequately authorized, deployed and maintained. It avoids access by unauthorized users, to protect network service; to prevent unauthorized computer access; and to prevent unauthorized access of information in the information system. At the same time, it can detect unauthorized activity and to ensure the information security during the utilization of portable computer operation and remote work facility.
(h) Systems development and maintenance: ensures that the information system has the security system established; prevents loss, alteration or misuse of information of users in the application system. It protects the confidentiality, availability and integrity of information, as well as ensures that the information technology project and support activity can be executed in a secured form. That maintains
the security of the application system software and information.

(i) Business continuity management: prevents interruption of the operation activity; and protects important operation process from being affected by major breakdown or disaster.

(j) Compliance: avoids violation of all criminal and civil codes, administrative order, management provisions or contract obligations and all security requirements. It ensures that the system can abide by the organization security policy and standard so that maximum result can be obtained during the system audit process and it can reduce the interruption generated or received during the course of audit to a minimum.

In this section we have addressed the control items within ISO 27001 to identify how it can be improve information security risk control.

3. The function of event manager

Nowadays enterprise sets a lot of security facilities to prevent the security threat. Generally, huge different format dialog comes from security systems (facilities) of different companies. Generally, there is no way to process the cross comparison and analysis, neither to find out the relationship between them. That will become as the heavy burden for the system manager as time goes by. In order to effectively manage these security information centralized and find out the existed defects and potential attacks to the system security, the enterprise should carry powerful monitoring and management ability to the security events. That can definitely provide remedies in short time. Security event manager system can be regarded as a kind of security monitoring system for managing a plural of heterogeneous information security facilities. The reaction ability to the security event can be enhanced via the processing of security event manager, although huge blog generated by the above independent systems. Besides that the security event manager system can real-time process the information collected from the security system and networking for the event management of security processing. That can help the management information systems (MIS) department more efficiently to response to the threats from both the external and internal environment. There are many matured products such as: RSA enVision, ArcSight ESM, Novell Sentinel, SPLUNK and OSSIM...etc. The processing flow is showed in figure 3 [9].

4. Attack methods and security technology

Regardless of whether information is stored in media (hard disk, magnetic disk) or is transmitted via network, it is possible to be attacked by people with intention. The present common methods and information security technology are explained as follows:

(a) Sniffer: sniffer computer system or network packets to collect required information. Substantially sniffer will not conduct real damaging attack or invasion, yet normally it is the preparation action before attack [10].

(b) Password cracking: refers to utilization of program or other method to crack the password. Mainly there are two methods to crack password including guessing the correct password or using brute force one by one to try all possible password. When guessing method is used to crack the password, it is possible that one dictionary file is required as auxiliary tool [11].

(c) Scanning: refers to scanning of the computer system to obtain the required information. Attacker will use scanning to get the information he wants to attack like Operating Systems (OS) version, what kinds of service are available, the provided service program and even the discovered pattern used to compare and find out loophole directly (such as: Cisco IOS version loophole).

(d) Malicious code: refers to that attacker will install malicious program to the system via external device or network and it can be divided into two types: virus and backdoor. Virus is a kind of computer program that can be self duplicated or operated without noticing or approval by user. Generally speaking,
under the condition unknown by computer user, the external communication program can be called as backdoor.

e) Denial of service: block certain service on the attacked machine so that legitimate users cannot access the system resource or information normally [12].

The well-known terms in security technology.

(a) Data encryption: data encryption is conducting a change on the information content through certain rules (such as: algorithm), so that the attacker cannot acquire the encrypted information and cannot obtain the correct information content [13].

(b) Virtual private network (VPN): VPN is a kind of utilization of tunnel and encryption method in the open Internet to establish a private and secure network [14].

(c) Intrusion detection system (IDS): IDS has the ability to make up the insufficiency of firewall. In general, firewall can only conduct limitation on the access of certain services but it cannot detect whether the entered packet is abnormal or not. The intrusion detection system can analyze the entered packet and compare with the established invasion trait database so as to examine abnormality and provide warning.

(d) Firewall: is a kind of device to assist in ensuring information security. According to specific rule, it will permit or limit the information passing through. Firewall may be a set of dedicated hardware or a set of software installed on the hardware. [15].

5. Information security blueprint

In the previous sections, introduction is conducted separately from the view of technology, flow and risk management to discuss about the enterprise information security separately. This paper presents a high level of perceive to consider more complete enterprise information environment. Once the plan is initiated it is required to obtain agreement from the management level and sufficient authorization. For information improvement and setting into motion that can be regarded as the most important step. Following is to establish a project team to carry out the entire information improvement planning. Not only members in the team should include information personnel, the team also requires the participation by personnel from different departments including risk managing personnel, audit personnel and legal personnel…etc. After acquiring the understanding of the management level and establishment of cross department project team, then the evaluation stage will be carried out. The contents include examination of the present information flow, risk management and information infrastructure…etc., so as to facilitate understanding on place of incompleteness within the present enterprise. It is suggested to carry out flow evaluation to understand the present IT management condition and to reduce the effect when ITIL is guided in and expense as well as manpower is put in. The Gartner IT Management Process Maturity Model can be divided into five steps [16]:

Step 1 Chaotic: there is no IT flow management neither document management inside the company. The IT department only plays the role in problem solving passively.

Step 2 Reactive: inside the company there are initial problem and flow standards including Incident Management.

Step 3 Proactive: under the ITIL architecture, IT department can provide service actively and conduct necessary change upon discovery of problem.

Step 4 Service: IT department becomes a service provider and can integrate various kinds of flows and monitor various kinds of Service Level Agreement (SLA).

Step5. Value: IT can combine with strategy of the enterprise and has commercial planning.

Following this and before the establishment of ISO 27001 – ISMS, three evaluation stages shall be carried out first:

(1) Listing the internal information asset of the company.
(2) Complete the risk evaluation on the information asset (risk evaluation is based on asset business and threats etc. and to appraise whether the present information security measures can conform to the requirement of the enterprise. If these cannot fulfill the requirements, evaluation will be conducted again on whether other security measure or method is required, for example: signing of maintenance contract, transferring the risk to information supply company etc.)

(3) List into the ISMS asset item according to its importance and the level of being threatened.

In the flawless enterprise information architecture, establishment of document system is very important. This paper suggests adopting ISO four stages document management system that is the standard for recording complete information.

An introduction to the ISMS document system

Establish management information according to ISO 27001 requirement and with complete document and record, it can ensure the abidance direction in the course of establishment and after completion and it can be divided into:

First stage document: security manual, policy declration, adequacy declaration …etc.

Second stage document: procedure that is used to describe the information of processing personnel and affairs.
Third stage document: work instructions that describe how to complete the work and activity.

Fourth stage document: records.

When the ITIL is guided in, as the fund and manpower of enterprise is limited, enterprise can start by guiding in “Service Desk”, “Incident Management”, “and Problem Management”. After the management can obtain its results, then other flows can be guided in.

Apart from enhancing the security of flows and risk management, adjustment of the information infrastructure is also important. There is an introduction on some attack methods and common information security facility before. In regard to integration, it is suggested to utilize the defense in depth method [17]. Its concept is to combine various kinds of different security defense systems to mutually make up for the inadequacy of individual security system in order to enhance the intensity of the defense. The suggested network infrastructure is as Figure 4.

![Figure 4. Network Infrastructure](image)

In the entrance of network, the IPS is established. Following this is the application layer firewall and IP layer firewall. In addition, the Server that the service provided to outside by the enterprise shall be placed in the perimeter zone (or called as the DMZ zone). Moreover, the internal server, personal computer and database are deployed with different network segment with utilization of firewall as the filtration system during passing through of packet. Furthermore, the endpoint protection firewalls, host intrusion detection system are added on various hosts that are used to protect the operation of host. Apart from increasing protective measures, the patch of the Operating Systems, software program, host authority limit and utilization authority limit control of database are also very important. Due to many heterogeneous systems existed in an information organize: the related log and alert are incompatible. It not only makes the efficiency of the enterprise low, but also increases the threats of security. The security event manager system in this paper can simplify and normalize the information comes from these systems. So that the valuable trend and event can be found and filter out the useless information. A better effect of security information concept can be achieved by periodic remind to all users.

After adjusting the entire enterprise information flow, risk management and infrastructure, as the enterprise operation and business direction may be adjusted and changed due to the change of time, therefore periodical review on relevant flows, risk planning and the information infrastructure shall be carried out in order to achieve the optimal result and the suggested flow is as Figure 5.

![Figure 5. Suggested guide in flow](image)

6. Conclusions

Information security is a problem that must be considered comprehensively. As long as problem appears on any segment, it will result in affecting the operation. These problems can be prevented or the effect can be reduced through a set of suitable control system. This set of system includes a series of management, flow improvement and architecture adjustment…etc. Enterprise is required to establish this set of system to ensure the materialization of specific security objectives and mission. Enterprise information security is to prevent information from receiving various kinds of threats and is used to ensure the business continuity so that the business risk can be minimized. In this paper, the ITIL and ISO 27001 are combined to improve flows and to reduce risk. By coping with the suggested information infrastructure adjustment, it is expected that optimal result can be achieved.
7. References


