Study on Applying ISO/DIS 27799 to Healthcare Industry's ISMS

[1] KWO-JEAN FARN, [1,2]JIANN-MING HWANG, [1]SHU-KUO LIN
[1]Institute of Information Management,
National Chiao Tung University,
No.1001 Ta Hsueh Road, Hsinchu, 300,
TAIWAN
[2] Department of Computer Science and Information Engineering,
Ming Chuan University,
No.5, Deming Rd., Gueishan Township, Taoyuan County 333,
TAIWAN
[1]kjf@iim.nctu.edu.tw, [2]jmhwang@mcu.edu.tw, [3]kuo@iim.nctu.edu.tw

Abstract: - At present, as healthcare sites use more and more IT system, information systems have come to play an important role in the business operation of healthcare organizations. It is an important goal for management at healthcare organization in Taiwan to keep the security of healthcare informatics. HIPAA had been run about ten years in USA, thought its efficiency has still remained to be seen, HIPAA has become the benchmark of the information governance in the information security of healthcare industry. The Department of Health of Taiwan had adapted from HIPAA and issued the HISPP/GD that included 9 principles and 12 articles altogether. This text will probe into the ISO/DIS 27799, the feasibility of applying it to the management of domestic healthcare organization and the corresponding detail of ISMS. By this way, we hope that Taiwan's healthcare organization could build a healthcare information system and manageable environment that according with the security requirements of confidentiality, integrality and availability.

Key-Words: - CNS[1], HIPAA, HISPP/GD[2], Risk Management, Information Governance, Healthcare Informatics Security, Information Security Management System (ISMS).

1 Introduction

In January 2001, the "Information & Communication Security Mechanism Plan" was approved in Council Meeting No.2718, and the "National Information and Communication Security Taskforce" (NICST) was established, to actively launch Taiwan's information & communication security infrastructure. After that, the certification of ISMS has already become the priority of information security in Taiwan. On the basis of cooperating with the demand for mutual trust among healthcare organ, relevant enterprise's partner and patient, the first two parties must look for the solution to offer the securities of information, trade and communication, and control all information materials correlated with the patient.

There are some good reasons for all participants to refer so as to promote and carry out the safety protection of healthcare informatics and electronic signature control: (1)Making the enterprise decision and relevant operation of healthcare organ better by the given informational and electronic capability; (2)Maintaining the personal and healthcare information, promoting the trust among patients and healthcare organ, avoiding the dispute, this is also a benefit of the healthcare information; (3)Abating the risk of the medical lawsuit, protecting enterprises of healthcare organ, this is also a chance to reduce the lawsuit among healthcare organ and patient; (4) According with the legal provisions, reducing the puzzlement distrusting with each other in lawsuit.

However, many healthcare organizations do not handle personal information such as patients' healthcare data as systematically as they do risk management for mistakes in healthcare practice. In addition, as healthcare sites use more and more IT system, information systems have come to play an important role in the business operation of healthcare organ. Since the shutdown of an information system would seriously affect healthcare services, controls are also required to deal with this. If information security cannot be maintained, many disadvantages will follow. Security management is vital if these disadvantages are to be addressed [Table1, page 2].

Table 1: Disadvantages arising from a failure to maintain information security

Poor medical services and loss of profits	A shutdown of the system will affect medical services and lead to the loss of medical service fees
A loss of trust and brand image	A loss of trust from patients as a medical organization
Repair costs required	The costs of time and work to recover the system will arise
Judicial action and claims for compensation	If information such as personal information or others is leaked, the injured party may bring a lawsuit for damages
Legal liability	The penalty clauses in the Medical Practitioners' Law, the Medical Service Law, and the Personal Information Protection Law

Table 2: Examples of the Items that Should Be Protected To Ensure Information Security

Types	Examples of Information Assets
Information	Patient data and medical service data in a computer system e.g. A patient's information written in that patient's file, request forms, or letters of introduction
Software assets	Operational application, system programs
Physical assets	Computer devices: computers, printers Storage media: MO, electromagnetic tape Communication equipment: networks, phones, and communication lines Electrical equipment: power cables, power generators, CVCFs
Services	Environment: machine rooms, whole buildings, and earthquake resistance functions
People (knowledge)	Knowledge such as medical information, operational know-how, and passwords

Table 3: Classification of the threats of information security

Threats			
Accidental Threats		**Intentional Threats**	**Environmental Threats**
Negligence	Failure	Crime	Disaster
Mistyping data Operational errors Wrong connections Others	H/W failures S/W failures Line failures Others	Stealing or tampering with information, Spoofing, Infiltration, Cyber terrorism, Viruses, Physical damage, etc.	Earthquakes Fires Water damage Others

Table 4: Examples of Vulnerabilities

Environment	Doors and windows, power supplies, site locations that can be stricken
Hardware	Aging and deterioration of driving parts, malfunctioning of backup circuits, etc.
Software	Missing specifications, access control failure, bugs in programs, etc.
Network	Not encrypted, protection error of communication lines, malfunctioning of backup circuits, etc.
Organization	Errors in educational programs, not-thorough managing third parties
Individual	Lack of skills, low morals, incorrect understanding, etc.

Table 9: PDCA model applied to ISMS processes

Plan (establish the SMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

ISO/DIS 27799 (Security management in health using ISO/IEC 17799) is drafted by ISO Technical Committee 215 (Health Informatics Working Group) in autumn of 2003 and under ballot as a Draft International Standard; ballot closes in October of 2006. It is based on BS-7799-2(CNS17800), ISO TR13335, and ISO/IEC17799-2000. Its main content is to apply ISMS to the management of healthcare information and to implement the healthcare security system with ISO/IEC 17799. Comparing to HIPAA, the domestic HISPP/GD has less contents, has not included the technical aspect, and has only the effect of promotion. In our opinion, the mentioned ISO/DIS 27799(announced by ISO), CNS 17799:2006 (issued by BSMI1, Taiwan) CNS 27001:2006 and other standards altogether can be regard as foundation of improvement and revision on HISPP/GD [Fig. 1].

The rest of this paper is organized into four sections. Section 2 states the adaptation of HIPPA. In section 3 and 4, applying ISO/DIS 27799 to healthcare information security and related issues are discussed. In section 5, conclusion will be addressed.

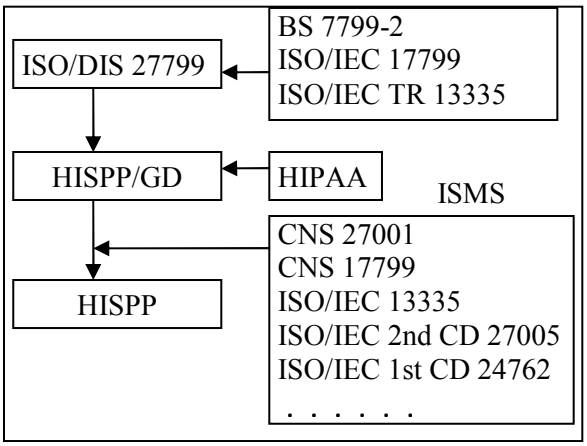


Fig. 1: Applying ISMS to HISPP/GD

Note:
(1)CNS (Chinese National Standards) administered by the Bureau of Standards, Metrology and Inspection (BSMI) of the Ministry of Economic Affair (M.O.E.A) of Taiwan
(2)HISPP/GD (Heath Informatics Security and Privacy Protection guideline draft, Taiwan)

2 HIPPA

The e-Taiwan Program is divided into 5 major parts: Infrastructure, e-Society, e-Industry, e-Government and e-Opportunity. The e-Taiwan Program is revised and evaluated regularly according to changing needs. E-Society promotes online education, entertainment, culture, health care, and transportation services, these initiatives will improve the quality of services avail- able to the public. HIPAA is adapted as the reference for creating the HISPP/GD that is an objective of e-health service inside e-Society program.

2.1 Reference of HIPAA

For the purpose of the regulation of information security and confidentiality and according with the requirement of privacy, the HIPAA (Health Insurance Portability and Accountability Act) is enacted by the U.S. Congress in 1996. HIPAA states the security mechanism for information system as follows: (a) administrative procedure; (b) physical safeguards; (c) technical security services; (d) technical security mechanisms. Comparing to HIPAA, the domestic HISPP/GD is less complex, only consider to strength the security control of healthcare informatics and patient's privacy protection in Taiwan's healthcare organization. All the time in Taiwan, how to achieve the goal of protecting the valid safety of healthcare information and patient's privacy in the healthcare organization, letting all participant personnel have the basis to legally and effectively implement the information controls and the protection behavior , have been worthy subjects to been probed into. The norm of HIPAA has been accepted by participants and covered entity of healthcare organization in U.S.A, while promoting the standard and regulation related to healthcare service in Taiwan, the regulation of HIPAA is worthy of referencing.

2.2 Application of HIPAA

Thought its contents is very different from the regulation of HIPAA, the HISPP/GD still keeps the relevant spiritual intension of HIPAA, such as the principle of minimum requirement that when healthcare organ collecting the patient's information should obey the rule of minimum necessary requirement as not to collect information other than healthcare usage. It also offer some other articles that according with the improvement of current Taiwan's healthcare society, such as the maximum security in reasonable scope principle for executing reference, because there is no definite standard for security, and it impossible to ask healthcare organ to unlimitedly budget for security, but only can ask them to evaluate security needs depending on their budget.

In October 2001, Legislative Yuan of Taiwan passes three readings of the Digital Signatures Law,

providing a legal basis for domestic e-commerce development and electronic information exchange. NHI (National Health Insurance) IC card that has the fundamental data and partial healthcare records of the patient, can be the media of communicating and exchanging of healthcare informatics. By combining NHI IC card with the standard of HL7 (Health Layer 7) and DICOM (Digital Image Communication in Medicine), various kinds of healthcare information can circulate smoothly among the healthcare organizations. The doctor uses medical personnel card, the patient uses NHI IC card and with the professional qualification authentication of the healthcare organ, this triple safety measures, can fill a guarantee that the privacy of patient's healthcare information is protected and communication security is safe. Under this situation, doctor and nursing staff use the computer properly, while carrying out the diagnosis and treatment they can quickly grasp patient's health status, understand the previous therapy situation and disease that patients suffering from. By this way they can avoid repeatedly examining, checking, and using medicine and get the result of economizing healthcare resources.

It is questionable according to numerous real cases that a lot of research projects or drafts ending up in nothing finally, would the HISPP/GD face this kind of destiny too? Since the "Health Safety " is a whole structure, if we want to achieve the following objectives at the same time: (a) to promote the medical society to strengthening and improving "Health Safety "(b) to carry out complete efficiency and improvement of the structure of both the patient and healthcare information security (c) to help the hospital to improve the existing medical careless mistake and the benefit of clinical warning system (d) to strengthen the realization and application of information security, then the integration of HIPAA, electronic case history, electronic health records, privacy and information security is essential in order to fulfill the demand of advanced patient security requirement. Hence, while drafting its policy and goal, the healthcare organization needs to build a patient-centric ISMS system that emphasis on using core standardized procedure foundation of the healthcare organization to the implementation of the steps and contents that stated in the standard. At the same time the healthcare organization need to audit and adjust procedure regularly, in order to construct a security mechanism that has compact association with patient safety.

For the purpose of information security and protection, while considering the construction of the structure of "healthcare informatics security policy", healthcare organization should base on the angles of structural and responsible aspects so as to build the fundamental layers of legal, organization, function, medical treatment, privacy, society, ethics and technology; and consider such directions as integrality, validity and accountability. By August 4, 2006, there have 132 private and public organizations in Taiwan passed the ISMS certification, but till January 1, 2007, still very few organizations have put "ISMS policy" in their ISMS document. In considering the ISMS policy of the "healthcare informatics security policy", healthcare organization should to set up and include both the "ISMS policy" and "healthcare informatics security policy"; In other words, ISMS should include "information security policy" and "ISMS policy"' at the same time.

3 ISO/DIS 27799

The ISO/DIS 27799(Draft International Standard) excerpts the following controls from ISO/IEC 17799: (a) Access control; (b) Information security policy; (c) Asset management; (d) Organizing information security; (e) Human resources security; (f) Physical and environmental security; (g) Communications and operations management; (h) Information systems acquisition, development, maintenance; (i) Business continuity management; (j) Information Security incident management; (k) Compliance. Its main content is to apply ISMS to the management of healthcare information and to implement the healthcare security system using ISO/IEC 17799. The partial cross-reference mapping table of CNS 17799 standard and HIPAA security standard is listed in Annex.

The following sections will narrate the steps and methods of how to construct and apply ISMS system to healthcare informatics security (HIS), the content of ISO/DIS 27799 that relative to the essentiality of HIS and the management of HIS, and the relevant weakness, threat, risk assessment and risk management of HIS.

3.1 Essentials of HIS and Its Management

One of the important points when managing Information security is to clarify "the purpose for which the HIS is being performed." It is important to define the objectives of HIS clearly, and manage security to achieve those objectives. The following are examples of some of the more important objectives: (1) Protecting Personal Information; (2)

Preventing Mistakes in Healthcare Practice; (3) Maintaining the Functions of the Healthcare Organs (The Continuity of Healthcare Services). The roles of healthcare organizations become greater in a major disaster. Even if the social infrastructure has suffered enormous damage, they must recover quickly and continue to provide healthcare services. They must also put in place suitable defensive measures to handle malicious attacks, to deal with problems such as cyberterrorism.

3.2 Vulnerability, Threat, Risk of HIS

Factors that cause risks are called "threats." More specifically, a threat is "a potential factor that causes a contingency that may result in loss of or damage to information assets or damage to the organization." A threat only becomes a problem when it has been occurred and has factors that cause actual damage. The weaknesses of the information assets that may elicit threats are called "vulnerabilities."; the vulnerability itself will not become a problem. A risk may be elicited by combining threats and vulnerabilities [Fig.2]

The following Assets: information, people (knowledge), physical, software and services, must been protected for information security. Table 2 is the listing of examples of the items that should be protected to ensure information security. Table 3 is the listing of classification of the threats of information security. Table 4 is the listing of examples of vulnerabilities [16, Page 2]

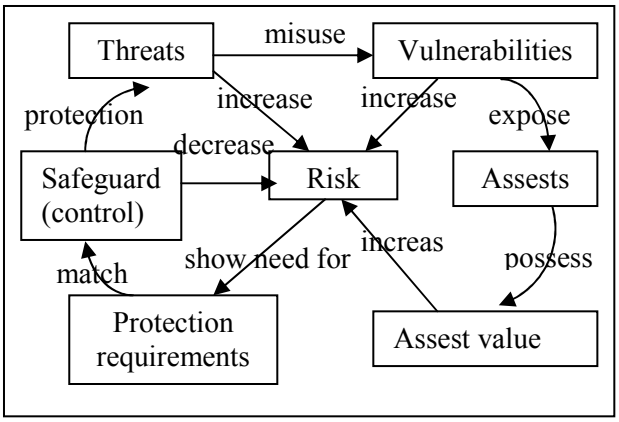


Fig. 2: The relation of Risk and Risk Resource [16]

3.3 Risk Management of HIS

Risk prevention means preventative measures that prevent a risk from occurring and is therefore especially effective for risks that cannot easily be dealt with via financial compensation. For example, it is easy to insure against credit cards forgery, but the large amount of damage caused by a leak of personal information (especially healthcare information) is difficult to cover with insurance alone. Measures for dealing with risks as follows: (a) Risk control: Using controls that help actively minimize damage. (b)Risk transfer: Measures to transfer risks to another company, e.g. by contract. (c)Risk retention: Measures for accepting risks as organization (d) Risk avoidance: Measures taken if no appropriate measures are found.

Table 6: Examples of calculation of the risk value of information assets

Elements of information assets	Value of assets
C: confidentiality	4
I: integrity	2
A: availability	1
Risk value = "value of information assets" ×"threats"× "vulnerabilities"	
threat 3 (if information is leaked to unrelated people, trust will be lost) vulnerability 3 (privileges are given to all operators)	
The risk value for this case is calculated as : Risk value for confidentiality: 4 × 3 × 3 = 36 Risk value for integrity: 2× 3 × 3 = 18 Risk value for availability: 1 × 3 × 3 = 9	

Table 7: Examples of the look-up score table of information assets

Information Assets	Threats								
	1			2			3		
	Vulnerabilities								
	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	8	18	27
4	4	8	12	8	16	24	12	24	36
	Range in which risks are acceptable (<9)								
	Range in which action should be taken to deal with the risk (>=9)								

3.4 Risk Management of Emergence Center

Emergence operation is critical for the patient's life, any disorder in the security or management of the back-up information system will cause disaster that causing death, losing of trust and brand image and causing claims for compensation. In the damage or risk analysis, the following three types are most fundamental: (a) potential damage type - such as earthquake, arson, etc. and evaluating the degree of

causing possibility and severity approximately; (b) impact degree of the damage - such as number of death, the amount of property loss; (c) response control – while aiming at the frequency and the severity of impact about damage, the constructed preparedness or responding strategy. In addition to obeying the general medical operation requirement, healthcare organ should implement risk assessment regularly in order to controlling the occurring possibility of risk to acceptable range.

While practicing the risk assessment of emergence center, we can produce an evaluation score table of risk matrix [Table 7] by following information: (a) the occurring possibility of the accident; (b) the impact (people, assets, business, preparedness, the internal and external responses, etc.); (c) threat, vulnerability and risk of information security. The score range could be (1~4), (A~E) or (1~100%), as described in Table 5[page 11], depending on the situation. There are many methods for calculating the risk value, the one stated in Table 6 is just for reference. If we set the acceptable (negligible) risk value as less than 9, then the darker area in Table 7 represents the unacceptable risk situation that the healthcare organ must to do some prevention control before accident happenings so as to control the occurring possibility of risk to acceptable range.

3.5 Framework of ISMS Policy Set

The policy of ISMS is defined as "the document record of ISMS decision" in this text. It is the instruction issued by high-level manager for the purpose of setting up ISMS plan, objectives and allocating the responsibility. The policy can be used to represent the specific security rule of special system, such as "business information system" and "access control system". It can also be used to represent the specific management decision of different issue of security policy, such as "Policy to manage information sharing", "privacy of personal information" and "Information exchange policies". Table 8 [page 11] is the listing the policies of ISMS which are explicit requirement in CNS 27001. Base on this, In addition to the "information security policy" and "ISMS policy" that are requirements of CNS 27001, ISMS also need to establish another two policies, "issue policy" and "system policy". The framework of "ISMS policy set" is depicted as Fig. 3.

In general, the "information security policy" and "ISMS policy" provides an ISMS plan that is in broader view and concerns about whole organization; the "issue policy" is focus on the controversial problem that is currently related to, being concerned by , and need to be solved by the organization . The definition of "system" of ISMS is "The whole collecting process for the purpose of executing the functionality of organization, including mechanisms that collect the manual data with man power or computer beforehand and the computer operation afterward". So the "system policy" of ISMS should be provided with two elements, "security objectives" and "operation security rule", which always attach to the steps and guideline while implement the policy.

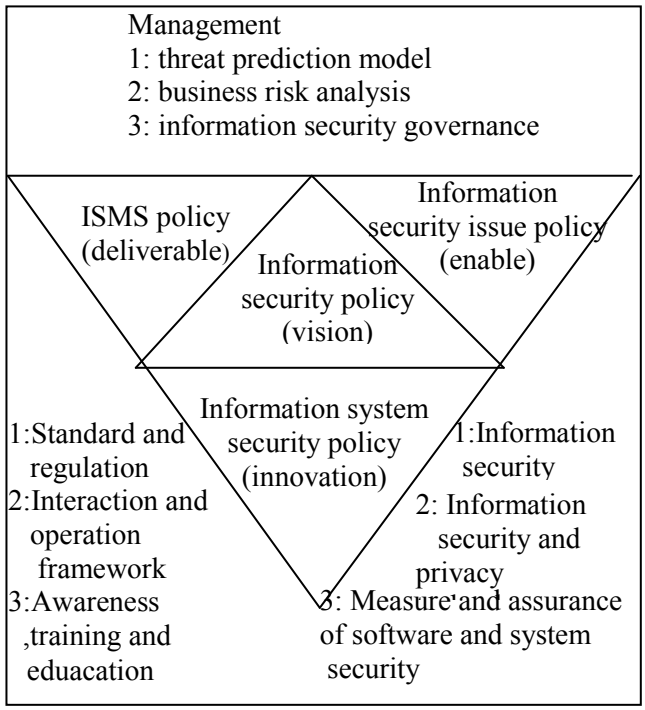


Fig. 3: Framework of ISMS Policy Set

"Policy" is the policy of "ISMS policy set"; it means the important decision related to information security. While making the decision the manager will have the following difficult selection: (a) resource allocation, (b) organization's strategic risk management context that related to information resource, (c) competitive objectives, information security assurance technology, (d) how to regulate the behavior of internal/external staff. Due to their authority, the "selection of policy" and the "applicability of the issued policy" by manager of different levels will be different. In general, the "information security policy" and "ISMS policy" should be issued by senior manager that has higher rank than CSO (Chief of Information Security Officer), since these two policies are generalized and need not to be modified in large scale in the future. The "issue policy" may need to be modified while the information technology and its related

factor has been changed, it is usually issued by senior manager, but when the policy becomes more complete, more controversial and more resource concerning, it should be issued by more higher level senior manager. The "Policy to manage information sharing", in the "business information system" is an example of "issue policy" in this category.

The "information security policy", "ISMS policy" and "issue policy" are advanced in the generalized view of whole organization and not the direction and information of implementation. For example, how to build a listing of access control [2] or regulate and teach the user that which behavior is allowable. On the contrary, the "system policy" of ISMS will fulfill this requirement, since it is against a specific system, has important impact on the usage of system and its security. The "system policy" is analyzed and evaluated by system technology management personnel and decided by high-level manager. The method for conducting the "operation security rule" from the "security objectives" is to adapt two levels modeling of system policies of "operation security rule" and "security objectives". For example, "All accounting voucher data after input to computer should be reserve forever, any modification should be eligible for accountability" is one "security objective" of financial system. After decision of this objective, we can conduct the following "operation security rule": (a) should define the authorized and unauthorized modification behavior for the incorrect input (b) operation rules of the financial information system (c) should this kind of modification be included in the sample population of audit work automatically or not ?. Since the adoption of "system policy" documentation is concerned with load of administration and implementation, the management should specify the detail. In general, access control document usually can make the "ISMS Policy Set" to implement and follow more easily [6, 10, 11, 14, 16, 17, 20, and 21].

4 Building the ISMS System of Healthcare Informatics

ISO/DIS 27799 is based on BS-7799-2(CNS17800), ISO TR13335, and ISO/IEC17799-2000. It builds the ISMS System of healthcare informatics by using the process model of PDCA (Plan-Do-Check-Act), as showed in Fig.4 & Table 9 [page 4]. The implementation detail is in the reference [1-3]. The system of healthcare security management, for example, managing problems with healthcare services, is built on the PDCA cycle.

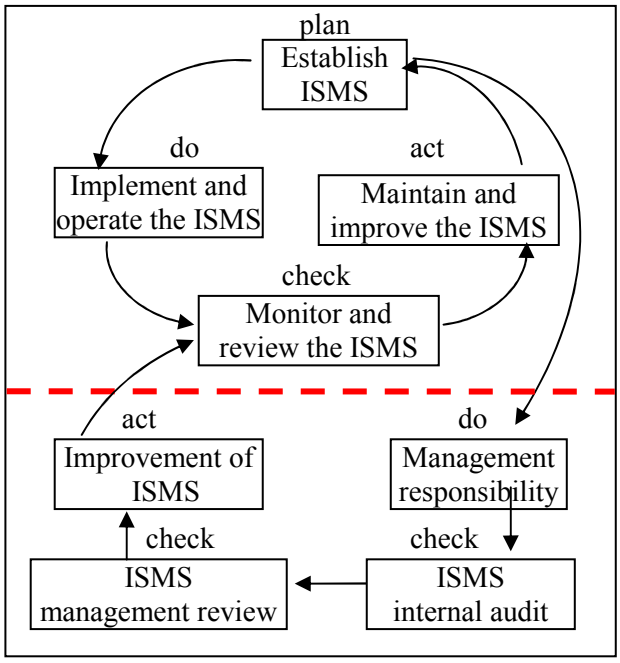


Fig. 4: ISMS process framework (PDCA)

4.1 PCDA Process Model of ISMS

CNS 27001:2005-10-15 is the improvement and update of CNS17800 (BS7799-2:2002), the digest of change for building and managing ISMS is as the following requirements: (1) the organization shall define the scope and boundaries of the ISMS and state the details and justification. (2) The ISMS policy is considered as a superset of the information security policy. These policies can be described in one document. (3) The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results. (4) Control objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection shall take account of the criteria for accepting risks as well as legal, regulatory and contractual requirements. (5) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results. (6)Monitor and review the ISMS should have the functionality as to help detect security events and thereby prevent security incidents by the use of indicators. (7)Measure the effectiveness of controls to verify that security requirements have been met. (8)Review risk assessments at planned intervals and review the level of residual risk and identified acceptable risk, taking into account changes to effectiveness of the implemented controls. (9)Update security plans to

take into account the findings of monitoring and reviewing activities

4.2 The Fundamental Elements of ISMS

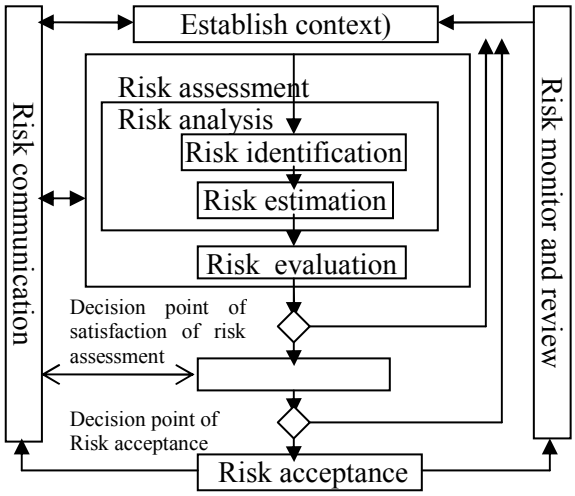
The follows are steps involved in establishing ISMS (1) Defining the range to which the ISMS apply – In terms of the characteristics, organization, location, assets, and technology of the business operation; (2) Planning ISMS policies – In terms of the assets, characteristics, organization, technology and location of the business operation; (3) Planning a systematic approach to risk assessment; (4) Identifying risks; (5) Performing risk assessment; (6) Performing risk treatment; (7) Selecting management goals and controls; (8) Preparing a Statement of Applicability. (9) Approving residual risks and allowing ISMS to be carried out.

One of the advantages of establishing ISMS is that security measures can be carried out with certainty. For achieving the objects of ISMS, this improvement is a part of the Act-Improvement process in the PDCA cycle, as showed in the lower part of Fig. 4 under the dotted line. It is important to continue to improve the effectiveness of the ISMS using the information security policy, information security goals, the results of audits, analysis of monitored events, corrective and preventive action and the output from management reviews.

As the idiom says "well begun is half done," the organization shall establish, implement, operate, monitor, review, maintain and improve documented ISMS within the context of the organization's overall business activities and the risks they face [2].

The "internal audits" control of ISO/DIS 27799 has been included in its "management reviews" section; we suggest that the "internal audits" control should be operated independently as in CNS 27001. Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself for internal purposes. The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS: conform to the requirements of this International Standard and relevant legislation or regulations; conform to the identified information security requirements; are effectively implemented and maintained; and perform as expected [1]. If nonconformities related to the way the ISMS is implemented or operated are found from the results of an audit and management review, actions must be taken to remove the causes of nonconformities and prevent them from reoccurring.

Preventive actions taken shall be appropriate to the impact of the potential problems [2]. Many healthcare organizations collect examples of tense moments or near misses in daily healthcare services and then analyze them, improve them, and, in particular, take preventive actions to prevent trouble. In the future, it will be vital to include trouble related to information security in these cases (of trouble) to analyze and improve them, if systems such as the NHI IC card system are to be carried out and used effectively in the future. It is important that risk managers consider these factors when taking preventive action.



1. Use the potential attack definition and quoted table of vulnerability analysis evaluation method of ISO/ IEC 18045 and attack reference path to establish the risk assessment situation of security object
2. Source:Guerin,F.(2006)Build CC assurance package dedicated to your risk assessment, Presentation to the 7th ICCC Conference, 2006-

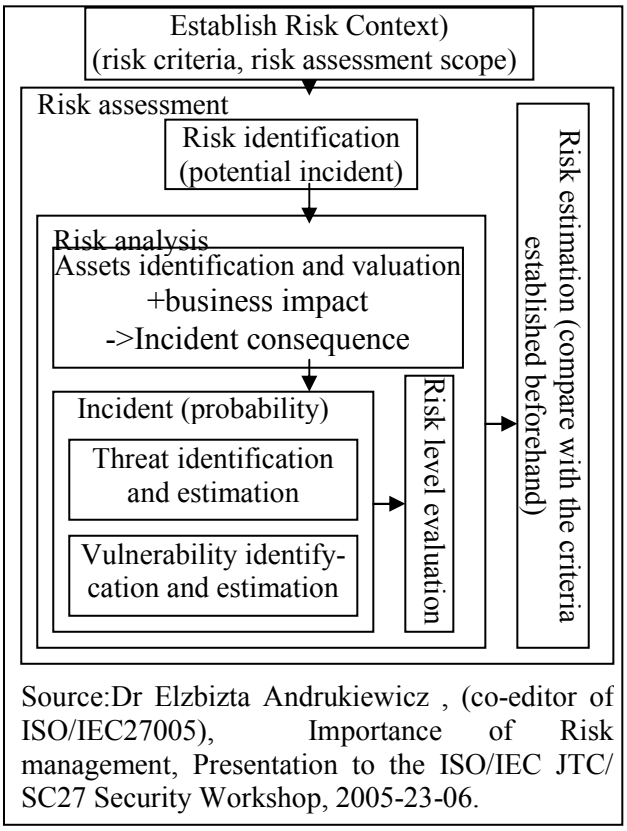
Fig. 5: Risk management process based on ISO/IEC 27005 and ISO/IEC 18045

4.3 ISMS Policy and Risk Management

"It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process and subsequently back to the ISMS policy and objectives." is the requirement stated in section 4.3.1 of CNS 27001 [ISO/IEC 27001:2005(E)]. Based on that, the core of ISMS policy is located in the veining of the context of risk management and risk assessment, as showed in Fig. 5 and Fig. 6 [1-4, 6, 13, and 14].

The ISMS is a system for all industries, always facing uncertainty. When management trying hard to create the value of information security for their

stakeholder, the challenge is dependent on how high the uncertainty that he/she will accepts. Uncertainty means risk or cost; the value of organization may be raising or falling because of it. The risk management of ISMS makes management to deal with uncertainty and the related risk and cost effectively, and let the organ to boost their ability of creating the value of managed information security.



Source:Dr Elzbizta Andrukiewicz , (co-editor of ISO/IEC27005), Importance of Risk management, Presentation to the ISO/IEC JTC/ SC27 Security Workshop, 2005-23-06.

Fig. 6: Image of Risk assessment process based on ISO/IEC 27005: 2007? (Under development)

ISM is operated in a changing environment of globalization, technology, organization, production, competition, regulation, and enactment. These factors cause the uncertainty of ISMS. Uncertainty could come from the happenings possibility in the future or the unknown result of an event/accident; or could come from the strategic selection of the ISMS policy; Such as the schedule and percent of the construction of DiD (Defense in Depth) [18], the requirement of "The Freedom of Information Law" and "Personal Data Protection Law", change of legislation etc. will influence the strategic selection of the ISMS policy and create the relative risk and cost; management use strategy to calibrate the risk appetite of organization and make it the same as the needs of organization[6].

Information security policy offers the necessary reliable foundation for the management and audit of ISMS; promotes more concernment and avoids the potential problems while implementing ISMS. The effectiveness of ISMS also involves the following topic: organization's business, operation threat and technical framework [12, 14, and 18].

Ensuring continuous management commitment is essential for accepting the structural processes of ISMS. Personnel need to recognize information security control and know how to do it, and to understand the benefit that this control will bring to organization. Generally speaking, unless supported by management, ISMS will be unsuccessful by itself. The Effectiveness measurements and indicators of ISMS provide the risk image of critical issue [Table. 10], let management to accept this concept and let organization willing to commit for supporting and maintaining ISMS. ISMS policy provides the implementation objectives for the effectiveness measurements and indicators of risk communication, risk monitor and risk review of the ISMS as stated in Table 11. Table 12 is the illustration of the retained reserves in Table 11. In sum of above, while organization is pursuing its mission or vision, the philosophy of considering its risk management and building its ISMS policy is depending on how much of risk the organ shall or willing to accept and how to alignment the strategic risk management context of the organization, In other words, under the same information security policy, an organization with different risk management philosophy, its ISMS policy and the retained reserves of its risk management sub-plan will be different[page 12, 13].

5 Conclusion

Security is like air, valueless in the beginning but becoming valuable while suffering from and losing it. The leak of privacy information causes unparalleled threat to Digital-Taiwan Program; time-consuming in verification, difficult in assessment, even there is a rumor that the china had hold the privacy information of Taiwan's people (tax/army data, and registered permanent residence). In March 2004, the event "Trojan horse's keylogger recording the account and password of cyberbank" had been noted in Taiwan. In April 2004, "Cross-strait hacker attacking office of president ROC," had been reported by media press. while ordinary becoming unusual, we shall recognize how to ensure the achievement of information security assurance by using the following method, "Information Operations (IO) that protect and defend information and information systems by ensuring their confidentiality, availability, non-repudiation,

authentication, and integrity, this includes providing for restoration of information systems by detection, incorporation protection, and reaction capabilities," is important segment of constructing the information security infrastructure of Digital-Taiwan, and is valuable public wealth.

The target of ISMS is "To Ensure the access of information resource is legal, to offer complete, uninterrupted operation of information system, in any stage that is possible for information attack." The security of information system is like a chain; its strength is depending on its weakest link. As showed in Fig. 3, the combination of information security policy, information security issue policy (Ex.: privacy policy), information system security policy (Ex. access control policy) and ISMS policy is the real source pool for hardening ISMS strength.

Based on CNS 27001:2006, CNS 17799:2006 and ISO/DIS 27799 and referenced on HIPAA, This paper probes into suggestion of the update and improvement of the HISPP/GD in Taiwan, and statement how to apply ISMS to healthcare informatics management and how to implement healthcare informatics security system. We deeply hope that this work will be some help to the management and security of healthcare informatics and let the people in Taiwan have better healthcare service and life.

References:

[1] BSMI-MOEA, ROC, *Information technology - Security techniques- Information security management systems-Requirements*, CNS 27001:2006.

[2] BSMI-MOEA, ROC, *Information technology - Security techniques — Code of practice for information security management,* CNS 17799 :2006.

[3] BSMI-MOEA, ROC, *Information Security Management Manual (draft)*, 2006.

[4] BSMI-MOEA, ROC, *The guideline for Risk Management, Vocabulary, standard usage,* CNS 14889:2005。

[5] BSMI-MOEA, ROC, *Information Technology Security techniques — Code for information security management*, CNS 17800:2002。

[6] COSO, *Enterprise Risk Management*, 2004,

[7] Department of Health- Executive Yuan, ROC. *Heath Informatics Security and Privacy Protection Draft,* http://www.cdrs.org.tw/ news_4

[8] Farn K.J., Lin Shu-Kuo, Lo Chi-Chun., *Study on ISMS Foundation Courses for Auditors?* WSEAS TRANSACTIONS on INFORMATION SCIENCE AND APPLICATIONS, Issue 10, Volume 3, pp. 1955 ~ 1962, 2006.

[9] Farn K.J., Lin Shu-Kuo, Lo Chi-Chun., *Study on the Network Isolation Security Requirements for Cyber Space?* WSEAS TRANSACTIONS on COMPUTERS, Vol.5, No.5, pp.1034~1040, 2006.

[10] Farn K.J., *Information Security Policy and Information Security system Policy (reference data)*, The Chinese Cryptology and Information Security Association, 2006.

[11] Geoff Skinner, Song Han, Elizabeth Chang, *A conceptual framework for Information Security and Privacy*,. Proceedings of the 5th WSEAS International Conference on Applied Computer Science, Hangzhou, China, April 16-18, 2006 (pp410-415)

[12] Howard, M. & D. Le Blanc, Writing *Secure Code* 2nd ed, Microsoft Press. 2004

[13] ISO, *Information technology - software life cycle processes - Risk management*, ISO/IEC 16085: 2004(E).

[14] ISO, *SSE--CMM* ®, ISO/IEC 21827: 2002(E).

[15] ISO, *Information technology – security techniques – Requirements for bodies proving audit and certification of information security management systems*, ISO/IEC 27006: 2007(E).

[16] JIPDEC, *ISMS User's Guide for Medical Organizations*, JIPDEC, pp1-77. 2004

[17] Kevin Beaver, Rebecca Herold, *The Practical Guide to HIPAA Privacy and Security Compliance*, Auerbach Publications, 2004.

[18] NSA (2002), *Information Assurance Technical Framework*, Release 3.1, 2002.

[19] Research, Development and Evaluation Commission-Executive Yuan, ROC, *Risk Management Operation Manual*, 2005

[20] Sheldon Borkin, The *HIPAA Final Security Standards and ISO/IEC 17799*, SANS Institute. 2003.

[21] U.S. 104th Congress, *Health Insurance Portability and Accountability Act*, Public Law 104-191, Aug.21, 1996,

[22] Ying-Ju Chen, Wender Lin, The Web Sites of Medical Centers in Taiwan, Proceedings of the 5th WSEAS International Conference on Applied Computer Science, Hangzhou, China, April 16-18, 2006 (pp653-657)

Table 5: Example standard of information assets

Assets	Class	Description
Confidentiality		
1(A)	Published	Can be disclosed and provided to third parties If contents were leaked, there would be little effect on medical operations.
2(B)	Internal Use	Can only be disclosed and provided in a hospital (not available to third parties) If contents were leaked, there would not be much effect on medical operations.
3(C)	Secret	Can only be disclosed and provided to specific parties and departments If contents were leaked, there would be a large effect on medical operations
4(D)	Highly confidential	Can only be disclosed and provided to specific parties If contents were leaked, there would be large or fatal effects on medical operations
Integrity		
1(A)	Unnecessary	Used only for reference. No possible problems.
2(B)	Necessary	If contents were falsified, there would be problems, but these will not affect medical operations very much
3(C)	Important	If integrity were lost, there would large or fatal effects on medical operations
Availability		
1(A)	Low	If the information became unavailable, there would be no effect on medical operations.
2(B)	Middle	If the information became unavailable, there would be some effect on medical Operations. However, alternative methods could be used for operations, or the process could be delayed until the information became available.
3(C)	High	If the information was not surely available when needed at any time, there would be large or fatal effects on medical operations .

Table 8: Information Security Management System and Policy

1. CNS 27001, section 4.2.1: Establish the ISMS
   - 1.1 Information Security Policy.
   - 1.2 Information Security Management System (ISMS) Policy.

2. CNS 27001, Annex A:
   - 2.1 A.5.1: Security Policy
   - 2.2 A.10.5: Information back-up
   - 2.3 A.10.8.1: Information exchange policies and procedures
   - 2.4 A.10.8.5: Business information systems
   - 2.5 A.10.8.5: Policy to manage information sharing
   - 2.6 A.11.1.1: Access control policy
   - 2.7 A.11.3.3: Clear desk and clear screen policy
   - 2.8 A.11.4.1: Policy on use of network services
   - 2.9 A.11.7: Mobile computing and communications policy
   - 2.10 A.12.3.1: Policy on the use of cryptographic controls
   - 2.11 A.15.1.4: Data protection and privacy of personal information

3. Class:
   - 3.1 Section Name: A.5.1, A.10.8.1, A.11.1.1, A.11.3.3, A.11.4.1, A.11.7, A.12.3.1.
   - 3.2 Control Statement: A.10.5, A10.8.5.
   - 3.3 The implementation guidance statement in section 10.8.5 and 15.1.4 of CNS 17799(ISO/IEC 17799:2005-06-15): A.10.8.5, A.15.1.4.

Table 11: Communication, monitor and review of risk management

	Process	Input	Used tool and technology	Output
Risk communication	Risk management planning	. Enterprise environment factors . Organizational procedure assets 3. ISMS scope statement 4. ISMS management plan	Risk planning and analysis meeting	Risk Management sub-plan
	Risk identification	1. Enterprise environment factors 2. ISMS scope statement 3. Risk inventory 4. Risk management plan 5. All rrisk management sub-plan	1. Document review . Information collection technology 3. Illustration technology 4. Checklist analysis 5. Hypothesis analysis	Risk inventory
	Qualitative risk analysis	1. Organizational procedure assets 2. ISMS scope statement 3. Risk inventory 4. Risk management sub-plan	. Risk probability and impact . Probability/impact risk rating matrix . Risk analysis data precision ranking 4. Risk analysis 5. Preemptive processing risk estimate	Risk inventory (updated)
	Quantitative risk analysis	. Organizational procedures assets 2. ISMS scope statement 3. Risk inventory 4. All rrisk management sub-plan 5. ISMS management plan . ISMS schedule management sub-plan . ISMS cost management sub-plan	. Information collection and presentation technology 2. Quantitative risk analysis and modeling technology	Risk inventory (updated)
	Risk response planning	1.Risk inventory .Risk management sub-plan	1. Active risk responses strategy 2. Passive responses strategy .Threat and chance responses strategy 4. accident risk responses strategy	1. Risk inventory (updated) . ISMS management plan (updated) 3. Law, regulation, contract articles relative to risk
Risk monitor and review	Risk control	1. Risk inventory . Risk management sub-plan . Approved request of change . Information of measurements and indicators of information security accident and event 5. Audit reports	. Risk inventory review 2. Risk re-assessment . Variance and tendency analysis 4. Measurements and indicators of information security accident and event . Retained reserves analysis 6. Current status review meeting	. Risk inventory (updated) . Request (changed) 3. Corrective control (suggested) 4. Preventive control (Suggested) . Organizational procedures (updated) 6. ISMS management plan (updated)
Source: A guide to project management body of knowledge, 2000 ed., PMI and this study				

Table 10: Image of information security risk contex

Consequence	Risk distribution		
Very serious	A2,C2	C1,L3,I1	I2,R1
Serious	L2	R2,A3	I3
Unserious	R2,L1	A1	C3
	Almost impossible	Possible probility	Almost sure

L= Legal or Regulatory environment, I =Integrity
R= Reliability, A=Availability, C=Confidentiality.

Table 12: Cost of ISMS risk management sub-plan

	Risk type	Risk process cost type
ISMS risk management sub-plan	known	corrective action
		preventive action
	unknown (including risk retention)	retained reserves
Source: A guide to project management body of knowledge, 2000 ed., PMI and this study		

Annex

[Note] The interpretation of the comparison symbol (>、~、<) of column "*" in the following table is based on CNS 17799:2006 (ISO/IEC 17799:2005)

CNS ~ HIPAA

For the topic of concern, the HIPAA and CNS requirements are approximately the same.

CNS > HIPAA

For the topic of concern, the CNS requirements include the HIPAA requirements as well as a substantial number of additional requirements.

CNS < HIPAA

For the topic of concern, the HIPAA standard includes at least one requirement not included in the CNS requirements. This designation may be used even if there are substantially more CNS requirements for the topic. The goal with this is to point out areas where the CNS standard does not fully contain the HIPAA standard

Table A-1: partial cross-reference mapping of CNS 17799 standard and HIPAA security standard

CNS 17799 standard	*	**HIPAA security standard mapping**
Introduction: Assessing security risks	>	Risk Analysis (164.308(a)(1)i)
Introduction: Selecting controls	>	Risk Management (164.308(a)(1)ii)
Management commitment of information security(6.1.1)	<	Assigned Security Responsibility (164.308(a)(2))
Information security co-ordination(6.1.2)	>	Information Security Activity Review(164.308(a)(1)i(D))
Allocation of information security responsibilities(6.1.3)	<	Assigned Security Responsibility (164.308(a)(2))
Identification of risks related to external parties (6.2.1)	~	Written Contract or Other Arrangement (164.308(b)(4))
Addressing security in third party agreements (6.2.3)	~	Written Contract or Other Arrangement (164.308(b)(4))
Information classification (7.2)	~	Accountability (164.310(a)(2)iii)
Roles and responsibilites(8.1.1)	~	Authorization and/or Supervision (164.308(a)(3)ii(A))
Screening (8.1.2)	~	Authorization Supervision Workforce Clearance Procedure (164.308(a)(3)ii(A)(B))
Information security awareness, education, and training (8.2.2)	~	Security Awareness and Training (164.308(a)(5)i)
.Physical and environmental security (9)		Physical Safeguards (164.310)
Physical entry controls (9.1.2)	~	Access Control and Validation Procedures (164.310(a)(2)iii)
Working in secure areas (9.1.5)	~	Authorization and/or Supervision (164.308(a)(3)ii(A))
Equipment siting and protection (9.2.1)	~	Workstation Use (164.310(b))
	~	Workstation Security (164.310(C))
Secure disposal or re-use of equipment	~	Disposal (164.310(a)(2)i) Media Re-use

(9.2.6)		(164.310(a)(2)ii)
Removal of property (9.2.7)	~	Accountability (164.310(a)(2)iii) Disposal (164.310(a)(2)i)
System planning and acceptance (10.3)	>	Information Security Activity Review (164.308(a)(1)i(D))
Protection against malicious and mobile code (10.4)	~	Protection Against Malicious Software (164.308(a)(5)ii(B))
Information back-up (10.5.1)	~	Data Backup Plan (164.308(a)(7)ii(A)) Testing and Revision Procedures (164.308(a)(7)ii(D))
Media handling(10.7)	~	Device and Media Controls (164.310(d)1)
Information handling procedures(10.7.3)	~	Accountability (164.310(a)(2)iii)
Electronic commerce services (10.9)	~	Mechanism to Authenticate Electronic Protected Health Information (164.312 (c)(2))
Monitoring(10.10)	>	Information Security Activity Review (164.308(a)(1)i(D)) Audit Controls (164.312 (b))
Monitoring system use (10.10.2)	>	Information Security Activity Review (164.308(a)(1)i(D))
Access control (11.)	>	Information Access Management (164.308(a)(4)i) Access Control (164.312 (a)(1))
Unattended user equipment (11.3.2)	~	Workstation Use (164.310(b))
User authentication for external connections (11.4.2)	>	Person or Entity Authentication (164.312(d))
User identification and authentication (11.5.2)	<	Unique User Identification (164.312(a)(2)(i))
	>	Person or Entity Authentication (164.312(d))
Password management system (11.5.3)	>	Person or Entity Authentication (164.312(d))
Session time-out (11.5.5)	~	Automatic Logoff (164.312(a)(2)iii)
Control of internal processing (12.2.2)	~	Mechanism to Authenticate Electronic Protected Health Information (164.312 (c)(2))
Cryptographic controls (12.3)	>	Encryption and Decryption (164.312 (a)(2)iv)) Encryption (164.312 (e)(2)ii)
Message integrity (12.2.3)	>	Integrity Controls (164.312(e)(2)i))
Key management (12.3.2)	>	Encryption and Decryption (164.312 (a)(2)iv)) Encryption (164.312 (e)(2)ii)
	~	Mechanism to Authenticate Electronic Protected Health Information (164.312 (c)(2))
Reporting information security events and weaknesses (13.1)	~	Response and Reporting (164.308(a)(5)ii(B))
Reporting information security events (13.1.1)	~	Protection from Malicious Software (164.308(a)(5)ii(B))
Collection of evidence (13.2.3)	~	Sanction Policy (164.308(a)(1)ii(C))
Information Continuity management(14)	~	Contingency Plan (164.308(a)(7)i)
Information security aspects of business continuity management (14.1)	>	Testing and Revision Procedures (164.308(a)(7)ii(C))
Including information security in the business continuity management (14.1.1)	>	Disaster Recover Plan (164.308(a)(7)ii(B))
Business continuity and risk assessment (14.1.2)	>	Applications and Data Criticality Analysis(164.308(a)(7)ii(D))
Business continuity planning framework (14.1.4)	>	Disaster Recover Plan (164.308(a)(7)ii(B))
Testing, maintaining and re-assessing business continuity plans (14.1.5)	>	Testing and Revision Procedures (164.308(a)(7)ii(C))
Prevention of misuse of information processing facilities (15.1.5)	~	Sanction Policy (164.308(a)(1)ii(C))
Technical compliance checking (15.2.2)	~	Evaluation (164.308(a)(8))