Industrial Engineering
& Management Systems
Vol 13, No 1, March 2014, pp.87-100
ISSN 1598-7248 | EISSN 2234-6473 |
http://dx.doi.org/10.7232/iems.2014.13.1.087

Development of a Failure Mode and Effects Analysis Based Risk Assessment Tool for Information Security

Lotto Kim Hung Lai
Hong Kong Science and Technology Parks Corporation, Hong Kong

Kwai Sang Chin*
Department of Systems Engineering and Engineering Management, City University of Hong Kong, Hong Kong

(Received: November 14, 2013 / Revised: February 25, 2014 / Accepted: February 25, 2014)

ABSTRACT

Risk management is recognized as a significant element in Information Security Management while the failure mode and effects analysis (FMEA) is widely used in risk analysis in manufacturing industry. This paper aims to present the development work of the Information Security FMEA Circle (InfoSec FMEA Circle) which is used to support the risk management framework by modifying traditional FMEA methodologies. In order to demonstrate the "appropriateness" of the InfoSec FMEA Circle for the purposes of assessing information security, a case study at Hong Kong Science and Technology Parks Corporation (HKSTP) is employed. The "InfoSec FMEA Circle" is found to be an effective risk assessment methodology that has a significant contribution to providing a stepwise risk management implementation model for information security management.

Keywords: Risk Management, Information Security, FMEA

* Corresponding Author, E-mail: mekschin@cityu.edu.hk

1. INTRODUCTION

Information security management involves systems, operations and internal controls by which the confidentiality, availability and integrity of data and knowledge of an organization can be assured. Information security aims to protect information from a wide range of threats so as to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security standards were initially released by the British Standard Institute (BSI) as BS 7799-part 1 in 1995 and became the ISO/IEC standard, i.e., ISO/IEC 17799, in 2000. Recently, ISO/IEC 27001-Parts 1 and 2 have been issued in 2005. It makes the controls required on this aspect clearly both locally and internationally. ISO/IEC 27001:2005 is directly related to the original BS 7799.

The history of the development of ISO 27001 is shown in Figure 1. In the beginning, UK Department of Trade and Industry was the first to develop the Code of Practice PD0003 on information security in September 1993, with assistance from a group of leading UK organizations. The code of practice was later re-titled and published as BS 7799-Part 1 "Code of Practice for Information Security Management" in February 1995 by BSI. BS 7799 provides a common basis for developing organizational security standards and effective information security management practices. It enhances confidence in inter-organizational dealings (Fung, 2004; Broderick, 2006; Barlette and Fomin, 2008). However, BS 7799-Part 1 was not widely employed in the industry for several reasons (Fung, 2004). Therefore, a new

standard BS 7799-Part 2 "Information security management system-Specification with guidance for use" was released in 1998. The structure of this standard is the same as Part 1. However, it defines a Code of Practice based on a set of key controls. Following the revisions of BS 7799 Part 1 in 1999, the standard was transferred to ISO/IEC 17799:2000 (Part 1)-Code of Practice for information security management. Finally, ISO/IEC 27001-Parts 1 and 2 were issued in 2005 and became more popular than the previous standards both locally and internationally. ISO/IEC 27001:2005 is directly related to the original BS 7799.

ISO 27001 was developed for protecting organizations' information assets since 2005. Up to 2008, 59 companies in Hong Kong have achieved ISO 27001 certification. The small number of ISO 27001 certified companies indicates the low adoption rate of implementing this international information security management standard (Fomin *et al.*, 2008). One of the key deficiencies of ISO 27001 information security management system (ISMS) has been identified to be lack of details on the methodology for risk assessment (Brenner, 2007; Fomin *et al.*, 2008; Misra *et al.*, 2007; Humphreys, 2008). It is recognized that risk management is a key element in the governance of an organization and in the protection of its information assets. If an organization does not know the risks it faces, it will not be able to implement proper and effective protection (Humphreys, 2008). Thus, one of the essential processes in ISO/IEC 27001 is to have an effective risk management system (Humphreys, 2008). This paper focuses on developing an effective risk assessment methodology for enhancing ISO 27001 implementation and to demonstrate the "appropriateness" for assessing information security.

In ISO/IEC 27001, the risk assessment approach of the organization is stated in the "Establishment of the ISMS" stage. Moreover, the risk assessment is reviewed at planned intervals in the stage of "Monitor and Review of ISMS." The proposed Information Security FMEA Circle (InfoSec FMEA Circle) is part of the ISMS PDCA (Plan-Do-Check-Act) model (see Figure 2).

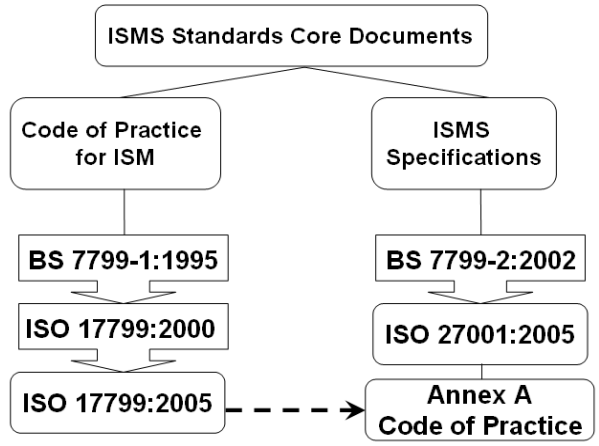

Figure 1. History of information security management system (ISMS) standards.

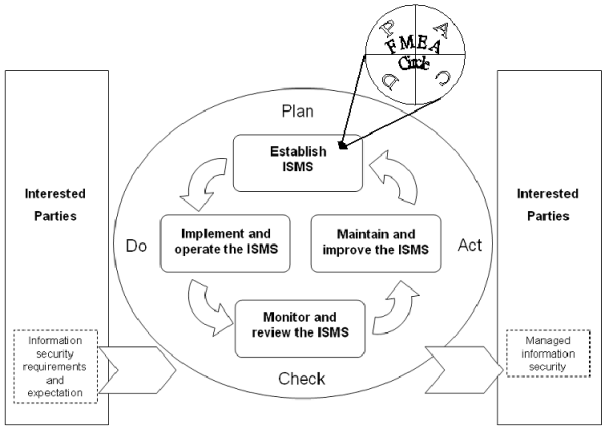

Figure 2. PDCA (Plan-Do-Check-Act) model applied to information security management system (ISMS) processes (ISMS model). Source: ISO/IEC 27001:2005.

1.1 Background and Project Justification

There is no regulation similar to the Sarbanes-Oxley Act currently available in Hong Kong (the Sarbanes-Oxley Act of 2002 was enacted as legislation in United States since 2002). Nevertheless, the Government of the Hong Kong Special Administrative Region (HKSAR) has issued a *Baseline IT Security Policy* and a series of guidelines related to information (IT) security that provide references and guidance to government bureau and departments on the protection of government information systems.

Unexpectedly, the major IT security incidents have occurred in Hong Kong since 2008. Some of them were (Hong Kong Computer Emergency Response Team, www.hkcert.org):

- Edison Chen's sex photos scandal (The Standard, 4 Feb. 2008).
- Hospital disclosed patients' personal information because of USB lost (Ta Kung Pao, 13 May 2008).
- Hong Kong Bank lost server which contained 159000 account information (Vivian Yeo, ZDNet Asia, 9 May 2008).
- Immigration Department leaked confidential information through Foxy software (Se San, Radio Free Asia, 18 May 2008).
- Usurious loan information were released through Foxy software from police.
- 69 policemen's information were leaked to public through Foxy software (Wenweipo [文匯報], 8 Mar. 2009).
- Hospital disclosed 47 patients' personal information because of USB lost again.
- Triad information were released through Foxy software from police (Computerworld Hong Kong, 3 Dec. 2009).

Incidents in banks, hospitals, immigration and police departments were found to be misconduct in handling sensitive information including loss of USBs and spreading of sensitive information outside the office area without control. They are not technical or operational control issues, such as network security or firewall configuration, but human error/misbehavior which should be under management control (Baker and Wallace, 2007). Why these incidents had always happened? According to studies of Humphreys ('father' of ISMS standards), surveys were conducted in the United States, UK, and elsewhere, and it found that 35% of security incidents occurring in organizations were caused by human errors or mistakes in handling data through careless working or lack of training, and this number of incidents is growing year by year (Humphreys, 2008). Therefore, ISO 27001 can be viewed as a solution which combines risk management, security management, governance and compliance to ensure the selection of adequate security controls that protect information assets (ISO/IEC 27001).

2. INFORMATION SECURITY RISK MANAGEMENT: A LITERATURE REVIEW

Risk management is recognized as an integral part of good management practice. To become a highly effective organization, company culture shall be developed to facilitate the adoption of risk management. Risk assessment and evaluation is currently one of the core elements in different management systems. For example, Occupational Health and Safety Management System (BS OHSAS 18001:2007) and ISMS (ISO/IEC 27001: 2005) employ risk assessment as a core element in those systems.

Due to the popular use of terminology of risk management given in ISO/IEC Guide 73, some crucial items and its definitions are captured as follows:

- Risk is a combination of the probability of an unfavorable event and its consequence.
- Risk Management System is a set of elements of an organization's management system concerned with managing risk.
- Risk Assessment is an overall process of risk analysis and risk evaluation.

Several national or international standards related to risk management were reviewed. They are AS/NZS 4360:1999; AIRMIC, ALARM, IRM: 2002; BS 31100: 2008; BS 31100:2011 and ISO 31000:2009 for generic risk; The ISO 27005:2011 was also reviewed which is specific to information security risk management. A number of risk management approaches from scholars, including Humphreys (2008), Misra *et al*. (2007), Tsohou *et al*. (2006), Kwok and Longley (1999), Spinellis *et al*. (1999), Halliday *et al*. (1996), and Baskerville (1991), were also studied and discussed. AS/NZS 4360 is a widely recognized risk management standard. This Joint Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee OB/7 on Risk Management as revision of AS/NZS 4360:1995-Risk management. Accordingly, it retains the objectives of providing a generic framework for establishing the context, identification, analysis, evaluation, treatment, monitoring and communication of risk (AS/NZS 4360:1999).

In Figure 3, the risk management overview described in AS/NZS standard consists of five stages: identification of context, identification of risks, analysis and evaluation of risks, identification and documentation of risk treatment. The four stages are described in terms of information security as follows (Misra *et al.*, 2007):

1) Identification of context, where the target system is described and assets are identified;
2) Identification of risks, where threats, vulnerabilities and possible unwanted incidents (attacks) are identified;
3) Analysis and evaluation of risks, where frequency of attacks and risks values are identified, and risks are prioritized; and
4) Identification and documentation of risk treatment, where the risk to be evaluated and its mitigated measures are identified. Those treatment actions should be documented.

In 2002, several organizations specializing in risk management in the UK, namely, The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and the National Forum for Risk Management in the Public Sector (ALARM), worked together to develop the risk management standard "AIRMIC, ALARM, IRM:2002" (Institute of Risk Management, 2002). This standard has enriched the AS/ NZS 4360 framework. According to the Institute of Risk Management (2002), there are a variety of views and descriptions of the risk management processes. A model for the three risk management stages, including initiation, risk analysis and risk mitigation, was adopted (Tsohou *et al*., 2006). The stage of initiation aims mainly to define the context of the risk management process; to set the scope of the analysis and to establish a risk management team. The stage of risk analysis involves the processes of risk identification, risk estimation and risk evaluation. In addition, there are three tasks included in the stage of risk mitigation:

- Design: including the security objectives and the establishment of security policies and processes relevant to control risk;
- Implement: involving the application of the selected control measures and procedures; and
- Monitor: ensuring the control measures are operating effectively and as intended.

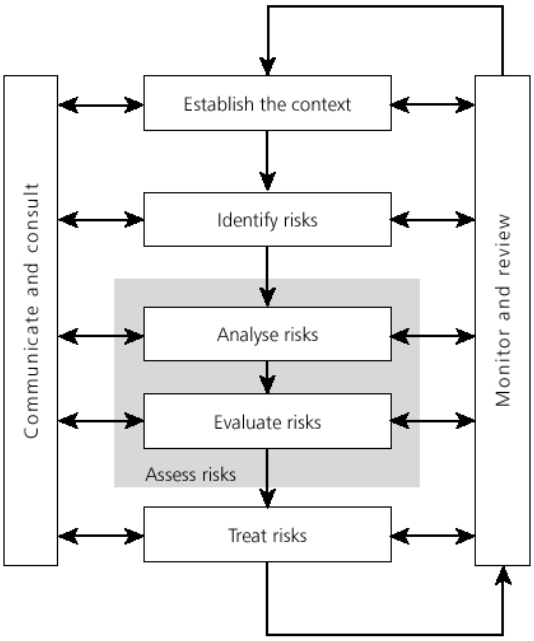

Figure 3. Risk management overview (Source: AS/NZS 4360:1999).

In order to establish the context, the scope and boundaries of information security risk management are defined. In risk assessment, the value of the information assets is required to determine, as well as the possible threats and vulnerabilities. To enforce risk treatment, actions and approaches should be selected based on the outcome of the risk assessment. There are four tactics for the purpose, including risk reduction, risk retention, risk avoidance and risk transfer. In fact, it is costly and not necessary to eliminate all risks. So, the acceptance level of residual risk should be established and endorsed by management. Exchange of information regarding the defined risks between the management and stakeholders is an important section. It could definitely be facilitated if information security risk communication is effective. Before the end of the loop, monitoring and review of risk factors should be carried out to identify changes to the context of the organization, if any, as early as possible, and to maintain an overview of the risk.

Moreover, ISO/IEC 27005:2011 was developed to give more details of the concepts and methods behind the risk assessment process, together with risk definition and classification for information security. It is more comprehensive than that in AS/NZS 4360. Hence, the results from the consideration of the likelihood of an incident scenario, against the estimated business impact are shown in Table 1. The risk scale uses a simple overall risk rating as low risk (0–2), medium risk (3–5), and high risk (6–8).

Risk management tools capture information in a consistent way, engage with stakeholders, and provide more thorough and reliable analysis results. They can be powerful aids to support effective risk management. In Table 2, an illustration of some of the most common used tools for risk management process is shown (BS 31100:2008-Table B.1). All listed tools were evaluated and classified into different analysis types, namely qualitative (QL), descriptive (D) and semi-quantitative (QN). Most of the risk management tools belong to qualitative and descriptive. Not surprisingly, failure mode and effects analysis (FMEA) was classified as semi-quantitative risk management tools.

The risk management tools' 13 selection criteria are stated in BS 31100:2008 (Annex B). They are based upon:

1) the intended user or function and the desired output;
2) the purpose or goal of undertaking the risk management activity;
3) the stage of the activity being undertaken;
4) the intended user's competence and experience with the tool's application;
5) the amount of time available for the risk study;
6) the level of detail that the sponsor requires;
7) the use to which the risk management outputs will be put;
8) the familiarity of the participants with the tools;
9) the degree to which risk management is embedded in the organization;
10) the willingness of the participants to use the tools;
11) the availability of information or data on the use of the tools in a productive way;

Table 1. Qualitative risk analysis matrix–level of risk (ISO/IEC 27005:2011–Table E.1b)

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Table 2. Examples of risk management tools

Tool	Identification*	Assessment*	Response*	Analysis type**
Risk questionnaires	x			QL/D
Risk checklists/prompt lists	x			QL
Risk management workshop	x	x		QL
Nominal group technique	x	x		QL
Risk breakdown structure	x	x		QL
Delphi technique	x	x		QL/D
Process mapping	x	x		QL
Cause-and-effect diagrams	x	x		D
Risk mapping/risk profiling	x	x		QL
Risk indicators	x			QL
Brainstorming/"thought shower" events	x			QL/D
Interviews and focus groups	x			QL/D
"What if?" workshops	x			D
Scenario analysis/scenario planning/horizon scanning	x	x		D
Hazard and operability study	x	x	x	QL
Failure mode and effects analysis	x	x		QN
PESTLE analysis	x	x		QL/D
SWOT analysis	x	x		QL/D
Stakeholder engagement/matrices	x		x	D
Risk register/database	x	x		D
Project profile model	x			QL
Risk taxonomy	x			D
Gap analysis: Pareto analysis	x	x		QL/QN
Probability trees		x		QL
Expected value method		x		QL/QN
Flow charts, process maps, and documentation		x		QL/D
Fault and event tree modeling		x		QL/D
Stress testing	x	x		QL
CPA or CPM		x		QL/D
Portfolio analysis		x		QL/D

PESTLE: political, economic, sociological, technological, legislation and environment, SWOT: strengths, weaknesses, opportunities and threats, CPA: critical path analysis, CPM: critical path method, QL, qualitative, D: descriptive, QN: semi-quantitative.

* The information of identification, assessment and response sourced from BS 31100:2008-Table B.1 (Table B.1 was removed in BS 31100:2011).

** Analysis types including QL/D/QN were classified by the author.

12) the ability of the intended user to understand the benefits of using the tools; and
13) the ease of use, suitability, cost and applicability of the tools.

ISO 31000:2009 is a new international standard for risk management. It provides principles and generic guidelines on risk management and can be used by any public, private or community enterprise, association, group or individual. It can also apply throughout the life of an organization, and to a wide range of activities, including strategies development and decisions making, operations and processes. Although ISO 31000:2009 is a generic guideline, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will have to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed (ISO 31000:2009).

The relationship between the risk management principles, framework and process given in ISO 31000:2009 is shown in Figure 4. It notes that the PDCA approach

and the process part is the same as AS/NZS 4360:1999; AIRMIC, ALARM, IRM: 2002; and ISO 27005:2011, which illustrates that ISO 31000:2009 has integrated different risk management standards together to form a generic guideline for various industries.

After reviewing different risk management models including AS/NZS 4360:1999, Institute of Risk Management (2002), ISO/IEC 27005:2011, BS 31100:2008, BS 31100:2011, and ISO 31000:2009, the basic principles of these standards are considered the same. Yet, the risk management process in ISO/IEC 27005:2011 is found to be more focused on information security aspects. Besides, two common key elements are concluded to be widely used in different risk management models. They are PDCA framework and four key stages of risk management process (Misra *et al.*, 2007).

However, there is no specific risk assessment tools recommended for ISMS. After reviewing the most commonly used tools for the risk management process, shown in Table 2, it was found that most of the risk assessment tools were qualitative and descriptive, in which the assessment of probability and consequence of a risk are expressed in a "Low/Medium/High" scale or its derivatives (ISO/IEC 27005:2011).

Apart from the qualitative and descriptive risk assessment tools, FMEA is a procedure by using which potential failure modes in a technical system can be reviewed. A FMEA can be extended to failure modes, effects and criticality analysis (FMECA). In a FMECA, each identified failure mode is ranked according to the combined influence of its likelihood of occurrence and the severity of its consequences, as well as the likelihood of the potential failure being detected. It is a semi-quantitative approach for risk assessment based on calculating the risk priority number (RPN). Therefore, FMEA was selected as the risk assessment tool in this study.

After reviewing different risk management standards and literatures, as well as risk management tools selection criteria, some benefits of using FMEA-based risk management were defined and are shown as follows:

1) Through FMEA, potential failure modes in a technical system could be reviewed. By computing an RPN to evaluate the level of risk, a comparative and semi-quantitative FMEA-based risk assessment method was preferred.
2) The desired output of information risk assessment is the potential hazard on information security issues and control mechanism. FMEA's potential failure modes identification and its control measures are suitable for the purpose of this study.
3) Staff's competence and experience are considered. FMEA is the fundamental technique for manufacturing industries and the staffs are already trained in most ISO 9001 certified companies.
4) The modification of FMEA is employed for information security. Therefore it could reduce the learning time for new risk assessment tools.
5) Finally, the ability to detect the potential failure modes is unique feature in FMEA and it was found to be very useful for automatic detection system in an information security network.

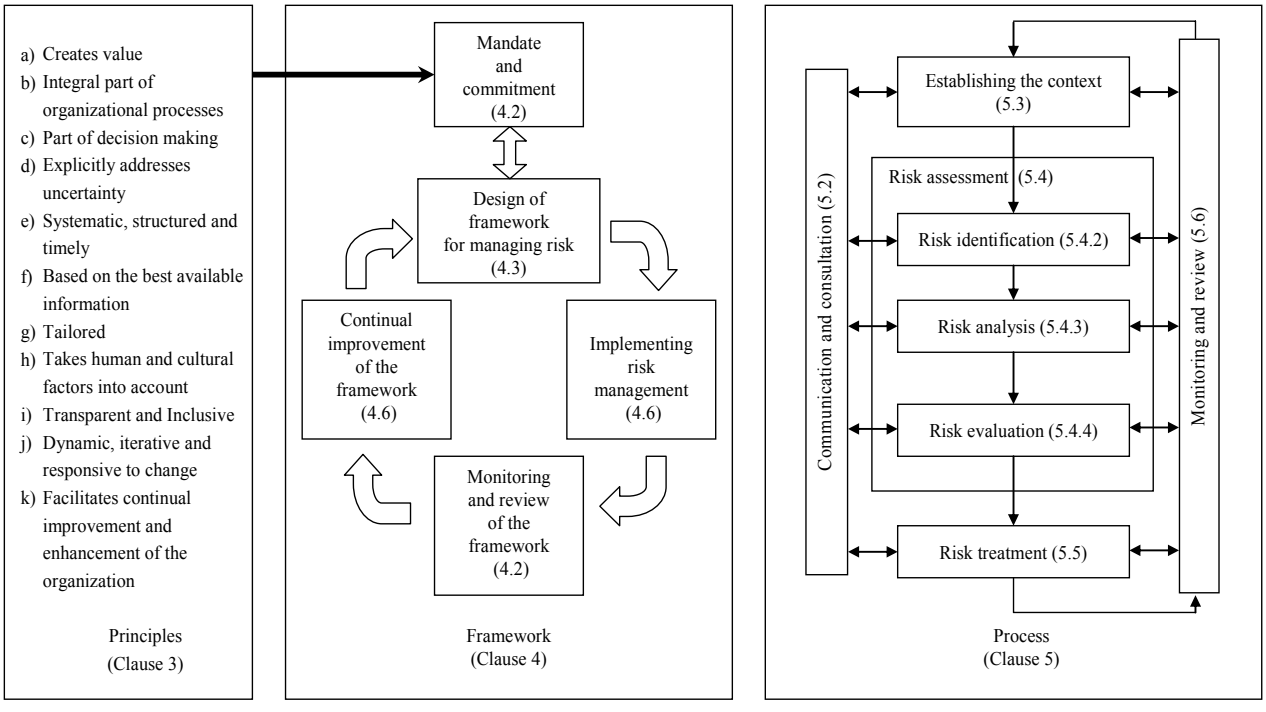

Figure 4. Relationships between the risk management principles, framework and process (Source: ISO 31000:2009).

Risk management for information security in ISO 27005 does not contain semi-quantitative risk assessment tools and ISO 31000 provides only a risk management framework (PDCA circle) and the associated process (4 key stages). FMEA was selected as a risk assessment tool for risk evaluation and it needs to extend to be risk management approach. Therefore, InfoSec FMEA Circle was developed to complete the risk management framework by modifying FMEA-based risk assessment tools and combining it with PDCA and risk assessment process to fulfill ISO 27001:2005 standard.

3. FMEA APPROACH (INFOSEC FMEA CIRCLE: THE THEORY AND IMPLEMENTATION MODEL)

A systematic approach to keep risks of information security under control is essential. Experts of an organization could define the requirements for securing their knowledge and information scientifically and create an effective ISMS. By review the system regularly, the approach could become a continual process. FMEA has the mentioned attributes to facilitate the analysis of a system so as to identify the potential failure modes, their causes and effects on system performance in terms of hardware, software and process.

InfoSec FMEA Circle is formulated by combining PDCA (ISO 9001:2008, ISO 27001:2005), risk management process (AS/NZS 4360:1999, ISO 27005:2011, ISO 31000:2009) and FMEA (IEC 60812). The conceptual model of InfoSec FMEA circle is described step by step in the PDCA framework as follows (Figure 5).

3.1 Step 1: Plan (Establish the Context)

3.1.1 Selection of information security component for analysis

Identification of context is a stage in which the target system is described and information assets are identified. In the PLAN step, the scope and boundaries of an organization for adopting the information security risk management should be defined. InfoSec FMEA is a tool mainly for information asset identification and risk elimination. Thus, confidentiality, integrity and availability of information are the basic elements to consider before determination of precautions. The Information Asset Evaluation Form is developed and shown in Table 3.

The Form (Table 3) helps calculating the CLASS ranking (the ranking of information asset security risk), based on the three basic components, “Confidentiality”, “Integrity” and “Availability”: Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or process; Integrity is the property of safeguarding the accuracy and completeness of information; and Availability is the property of information being accessible and usable upon demand by an authorized entity.

The ranking scores are defined as follows:

1) Low effect ranking score is 1, indicating no significant impact to the business.
2) Moderate effect ranking score is 2, indicating a slight interruption of business activities but it will not cause litigation.
3) High effect ranking score is 3, indicating a great interruption of business activities that will cause litigation.

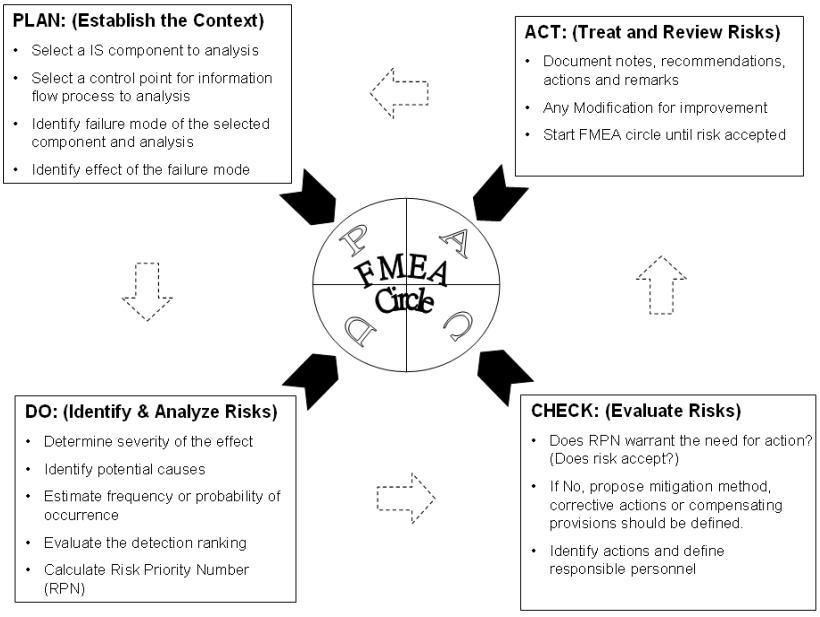

Figure 5. InfoSec FMEA Circle. FMEA: failure mode and effects analysis.

After using the evaluation form, the information security ranks can be categorized into 3 classes and they are:

1) Class A: The failure of the information asset is a very hazardous, which will cause high portion in loss of service/stop of service;
2) Class B: The failure of the information asset would cause some minor disruption to the whole service/process; and
3) Class C: The failure of the information asset would causes staff/customer experiences discomfort.

Those class rank and asset number are recorded into the InfoSec FMEA Form for traceability (see Table 4). The column F in the Table 4 showed the class and information asset code.

3.1.2 Selection of control point for information flow processes

An InfoSec FMEA can be applied for any information asset issue/project process and service flow. Table 4 is an example of InfoSec FMEA Form. It can be used to collect information of components and processes/functions through a team of engineers. After that, the 133 control points given in ISO 27001 Annex should be considered as the basic requirements to evaluate any potential information risk. As processes cannot be operated without information, the evaluation should then be extended to all other process flows. All information is recorded in column A and B of the form.

3.1.3 Identification of the potential failure mode on the selected control points/processes

After a list of control points and processes are generated, FMEA team (a group of engineers from different disciplines of the company) should move to define the relevant potential failure mode. Exchange of views should be encouraged. Potential failure mode is defined as the manner in which the process could potentially fail to meet the process requirements and/or design intent. It is a description of non-conformance for the specific operation (see Table 4-Item C).

3.1.4 Identification of the effect on the potential failure mode

The FMEA team shall further determine the Potential Effects if such failure occurs at each control points and processes (see Table 4-Item D).

Table 3. Information asset evaluation form

ITEM: Information asset evaluation form
CORE TEAM: AAA, BBB, CCC, DDD, EEE, FFF
PREPARED BY: AAA, BBB

CONTROL NUMBER / REVISION : QS_IAE_001
DATE: XXXXXX

Information Asset Evaluation Form

Asset no	Asset	Confidentiality	Integrity	Availability	Class rankin	Class	Asset owner
	Information/ Data asset (related to customer)						
1	Customer information (email, contract, etc)	3	2	2	**12**	**B**	Engineer, CSO
2	Customer IP, database, design/ project	3	3	3	**27**	**A**	Engineer
	Information/ Data asset (related to Centre)						
3	Staff information	2	1	1	**2**	**C**	HR
4	Contracts and agreements	3	3	2	**18**	**A**	Sr. Mgr, ADM
5	System Documentation (EDS)	2	2	2	**8**	**B**	QS
6	User manuals	2	2	2	**8**	**B**	Engineer
7	Audit trails	3	2	2	**12**	**B**	Engineer
	Technology asset (software)						
8	Application software (word, excel, etc.)	1	2	2	**4**	**C**	IT
9	System software (OS, etc)	1	2	2	**4**	**C**	IT, engineer
10	Development tools (EDA tools)	3	2	2	**12**	**B**	Engineer
	Technology asset (hardware)						
11	Servers, computer equipment	3	2	3	**18**	**A**	Engineer
12	Office equipment, fax machine, copier, printer, scanner, projector	2	2	2	**8**	**B**	CSO, IT
13	Networking and communications equipment	3	3	2	**18**	**A**	Engineer, IT

1 = no significant impact to our business
2 = slight interruption of business activities - will not cause litigation
3 = great interruption of business activities - will cause litigation

Table 4. InfoSec FMEA form

INFORMATION SECURITY POTENTIAL FAILURE MODE AND EFFECTS ANALYSIS (Info-SecureFMEA)

ITEM: ISO27001 Control Objective A.5 to A.15
CORE TEAM: AAA, BBB, CCC, DDD, EEE, FFF
PREPARED BY: AAA

CONTROL NUMBER / REVISION : QS_FMEA_001A
DATE: XXXXXX

A	B	C	D	E	F	G	H	I	J	K	L	M	N	
Clause No.	PROCESS FUNCTION / REQUIREMENTS	POTENTIAL FAILURE MODE (FAULT)	POTENTIAL EFFECT(S) OF FAILURE (IMPACT)	SEV	CLASS	POTENTIAL CAUSE(S)/ MECHANISM(S) OF FAILURE	OCC	CURRENT PROCESS CONTROLS (PREVENTION)	CURRENT PROCESS CONTROLS (DETECTION)	DET	RPN	RECOMMENDED ACTION(S)	RESPONSIBILITY & TARGET COMPLETION DATE	ACTIONS TAKEN & EFFECTIVE DA
7.2.1	Classification guidelines	1.Misclassification of information 2. No classification	Leakage of confidential information	8	B	5 1. No guideline in classification 2. Misuse of guideline 3. No clear document/ guideline	4	1. Confidential information is already defined in NDA 2. Confidential information is identified with chop	N/A	?	224	Follow the classification guide in ISMS SQM, 1 Dec 2007	ICDC/ IPSC	(classification of i employed) 12/7/2007

FMEA: failure mode and effects analysis.

3.2 Step 2: Do (Identify and Analyze Risks)

3.2.1 Determination of the severity of each effect on the respective potential failure mode

Severity is an assessment of the seriousness of each effect of a potential failure mode. The ranking ranges from 1 to 10, which represents the different degrees of an effect. The FMEA team should determine the effect of each potential failure mode based on the definition from "Hazardous-without warning" to "No effect", which corresponds to 10 and 1, respectively (see Table 4-Item E).

3.2.2 Identification of the potential cause

The FMEA team should, based on their knowledge on the product/process/services, list conceivable failure causes assignable to each potential failure mode. If causes have a direct impact on the respective failure mode, next action should identify the process controls in the FMEA correspondingly (see Table 4-Item G).

3.2.3 Estimation of the frequency or the probability of occurrence on each potential failure mode

Occurrence estimates the probability of a specific failure cause/mechanism occurring based on the historical data and experience, during the lifetime of the scope. The occurrence ranking number has a meaning rather than a value. Occurrence is usually rated on a scale from 1 to 10, with 10 indicating that failure is almost inevitable. The lowest occurrence ranking number is 1, signifying that failure is unlikely or not ever having any associated failures. In the case study, 10 and 1 imply the occurrence rate is less than 1 day and longer than 2 years, respectively (see Table 4-Item H).

There are two types of process controls to be taken into account (see Table 4-Item I and J):

i) Prevention: Prevent the cause/mechanism of failure or the failure mode from occurring, or reduce their rate of recurrence; and
ii) Detection: Detect the cause/mechanism of failure or the failure mode, and lead to corrective action(s).

The preventive measures at process control points will reduce the probability of occurrence of the potential failure mode (see Table 4-Item I).

3.2.4 Evaluating the ability to detect a potential failure mode

Detection is a relative ranking, within the scope of the Information FMEA, to estimate how well the controls can detect either the cause or its failure mode after they have happened but before the customer is affected.

Detection rankings shall be considered as follows.

- To achieve a lower ranking, generally the planned process control has to be improved.
- Do not automatically presume that the detection ranking is low because the occurrence is low, but do assess the ability modes or prevent them from going further in the process.
- Random quality checks are unlikely to detect the existence of an isolated defect and should not influence the detection ranking.

Detection is usually rated on a scale from 1 to 10 continuously. The higher the ranking, the lesser the failure can be detected. For the highest ranking (10), it means that the control is certain not to detect the failure mode or cause (i.e. no control exists). Oppositely, the lowest ranking (1) means 100% confidence on detecting failure mode or cause of the concerned system/process (see Table 4 - Item K).

The current process control measures for detection will reduce the detection ranking on the potential failure mode (see Table 4-Item J).

3.2.5 Calculation of risk priority number

RPN is the product of severity (S), occurrence (O) and detection (D) rankings (see Table 4-Item L).

$$RPN = Severity\ (S) \times Occurrence\ (O) \times Detectability\ (D) \quad (1)$$

RPN is calculated for each potential failure mode so that the most important failure mode with the highest RPN number can be subsequently found.

3.3 Step 3: Check (Evaluate Risks)

With the aim of providing guidance for ranking potential failures in order, a RPN is created. An acceptable risk level that is also called RPN level shall be defined. To visualize it, the implementation team could draw a line on the InfoSec FMEA Form based on RPN number. Simple techniques can be used iteratively for determining the acceptable risk level (RPN level). Apart from a professional team, the result could also be verified with front line staff and customers.

There are two decisions to be made based on RPN level. They are shown as follows.

1) If RPN > acceptable risk level, recommended actions should be performed for control purpose; If RPN < acceptable risk level, management needs to acknowledge the risks and accepts them (see Table 4-Item M).
2) If RPN > acceptable risk level but cost is too high to avoid it, some structural change may be required to mitigate them for keeping the cost acceptable.

When the failure modes have been ranked by RPN, corrective actions should be performed if the RPN is higher than 100 on critical items. The highest score of RPN is 1000 (10×10×10) and the acceptable level of RPN is set to 100 (means 10% of the highest score) (Lai, *et al.*, 2010). This acceptable level of RPN is based on

focus group in the HKSTP IT Security team decision. If an RPN larger than 100 which could occur in three situations with possible happen: Catastrophic Failure and semi-auto detection, when S = 10, O = 2 and D = 5; Routine low risk but manual handling, when S = 1, O = 10, and D = 10; and middle situation, when S = 4, O = 5, and D = 5, etc. However, RPN level will be different in different company and depends on industry. Information asset classification was also considered in those critical items. Even if an RPN is slightly below 100, recommended actions should also be implemented for the potential failure modes of any information asset belonged to Class A.

3.4 Step 4: Act (Treat and Review Risks)

The acceptable risk level of InfoSec FMEA circle is part of the continual improvement process. That means the acceptable risk level will be changed in the future as the business environment changes. After rating each potential failure mode based on RPN, any items which were above the risk acceptance level (i.e. larger than 100) were used to establish a risk treatment plan (RTP) for follow-up actions. The intent of any recommended action is to reduce the severity, occurrence, and/or to enhance detectability (see Table 4-Item M).

The responsible personnel and target completion date for each recommended action should be recorded (see Table 4-Item N). After corrective actions have been identified and executed, the degree of severity, occurrence and detection should be re-assessed (see Table 4-Item O).

The InfoSec FMEA of all processes should be reviewed annually. It should also be evaluated any time and revised as appropriate if the examined process is changed, becomes unstable or incapable.

4. IMPLEMENTATION OF INFOSEC FMEA CIRCLE

Information Security Risk Management involves a high number of human activities which influence various stakeholders. InfoSec FMEA Circle implementation is connected with all risk management elements such as risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review through the PDCA framework. It illustrates the relationship between the selected controls to the results of the risk assessment and risk treatment process. “Control objectives and controls” in ISO 27001 Annex can be selected and taken to meet the requirements identified in the risk assessment and risk treatment process.

The whole circle can be demonstrated by modifying Eq. (1) as follows.

$$RPN_{vi} = Severity\ (S_i) \times Occurrence\ (O_i) \times Detectability\ (D_i) \quad (2)$$

where v is number of processes and i is number of control points.

For example,

First cycle of InfoSec FMEA Circle,

v = 0, representing control objectives and controls in ISO 27001 Annex; and

i is from 1 to 133, indicating the 133 control points.

Second cycle of InfoSec FMEA Circle,

v = 1, representing operation information flow in process 1; and

i is from 1 to n(1), indicating the n(1) control points.

Third cycle of InfoSec FMEA,

v = 2, representing operation information flow in process 2; and

i is from 1 to n(2), indicating the n(2) control points.

…

M cycle of InfoSec FMEA Circle,

v = M, representing operation information flow in process M; and

i is from 1 to n(M), indicating the n(M) control points.

There are M InfoSec FMEA Forms created after reviewing all processes (see Figure 6)

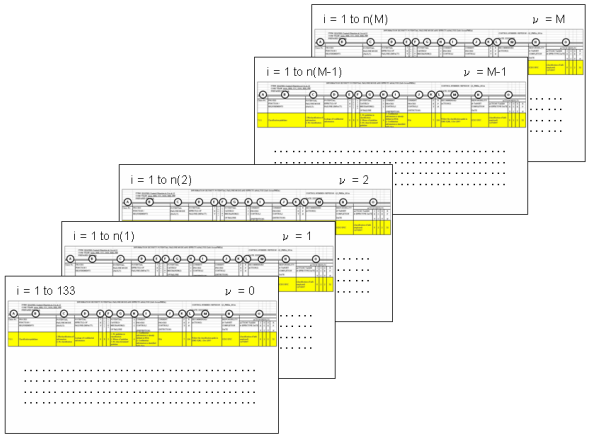

Figure 6. InfoSec FMEA Forms after M cycles. FMEA: failure mode and effects analysis.

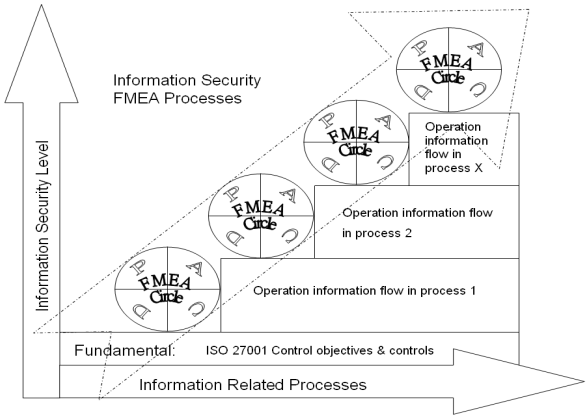

Figure 7. InfoSec FMEA Circle implementation. FMEA: failure mode and effects analysis.

After the RPN of each control is prioritized, the risk treatment should be performed for items with RPN greater than the risk acceptable level. However, for InfoSec FMEA, two prioritization levels were employed: the RPN rank and the information asset classification. It implies information asset classification will be considered for prioritize the risk if there are items having the same RPN.

Figure 7 shows the implementation of InfoSec FMEA circle. The fundamental stage is ISO 27001 "control objectives and controls." Then the FMEA circle goes through the operation information flows in each process, and finally it moves to the highest information security level systematically.

InfoSec FMEA Circle is implemented inside the 12 elements in the safeguard ring of the QMS based Information Security Management (QISM) Model. The safeguard ring involves fundamental ISO 27001 control objectives and they are "Security Policy", "Organization of Information Security", "Asset Management", "Human Resources Security", "Physical and Environmental Security", "Physical and Environmental Security", "Communication and Operations Management", "Access Control", Info System Acquisition", "Information System Incident Management", "Business Continuity Management" and "Compliance." After 133 control points in the safeguard ring are evaluated, InfoSec FMEA Circle is repeated for another operation process until all processes have been evaluated, it aims to reduce any remaining residual risk or vulnerability to an acceptable level.

The development of "Information Security FMEA Circle" can provide solutions to overcome the insufficiencies of FMEA stated by different scholars (Chin *et al.*, 2008, 2009; Wang *et al.*, 2009; von Ahsen, 2008; Segismundo and Miguel, 2008; IEC 60812:2006) below:

1) The proposed FMEA-based risk assessment sets the risk acceptable level below or at the score of 100 (that is 10% of the maxima score of 1000). Even though RPN is heavily distributed at the bottom (say below 100), the Information Asset Classification shall also be considered. If it is in Class A, more attention shall be given during system review.
2) Development of the evaluation method for Information Asset Classification based on Confidentiality, Integrity and Availability, it enhances the prioritization of RPNs if items having the same number of RPNs were obtained.
3) Since the acceptable risk level was suggested to be set at 100, the sensitivity of small change is not significant. Moreover, the Information Asset Classification is added as an important indicator for further consideration on which items should be included for correction or improvement.
4) The scaling system for evaluating of severity, occurrence and detection is from 1 to 10. Scale of each item was evaluated through discussion in a focus group, based on internal experts' experience and past data. Therefore, it has overcome the inadequate scaling.
5) Economic aspect is out of the scope in this study. It is because the information security is the most critical aspect in IT business.
6) For information security, many monitoring and checking steps will be specified and performed automatically through the IT system. RPN is always assessed by "Detection."
7) Even if there is an absence of a standard guide to determine the probability of occurrence (O) and detection (D), focus group interview can help to map out the definition of each score in occurrence (O) and detection (D).

5. CASE STUDY (RESULTS AND DISCUSSION)

In the IC design and semiconductor intellectual property (IP) industry, electronic design automation (EDA) tools and customer IP are the most important assets. Thus, an isolated network to protect license of EDA tools and customer IPs was expected. However, the tradeoff is to limit the number of customers to use the service (either working in our engineering room or connect optical fiber link within Science Park area). Currently, customers are required to upload their design data into the centre's system in a separate engineering room in ICDC and IPSC offices, with private networks setup before using the service provided by ICDC or IPSC. Although the degree of protection fulfills the application, customer's expectations are increasing with the rapid growth of internet technology. They requested that data uploading operations can be done remotely. So, customers could finish the task quickly in their work place, instead of assessing ICDC or IPSC offices physically. The following describes how we dealt with the tradeoff between customer's expectation increase and security requirement.

It is believed that a remote access system could serve a large number of customers simultaneously. However, the protection of IP right is of high concern to users and affected parties (IP suppliers). As a result, the creation of a Secure Virtual IP Chamber was decided as one of the business strategies. The highest risk identified in the remote access system was customers who access the chamber using virtual personal network. So, information security level in this area should be the highest. As mentioned, ISO 27001 standard was confirmed to be suitable for this situation and it is recognized internationally in the IT industry. It aimed to strengthen IP suppliers and users confidence in working in HKSTP. Furthermore, it could improve the overall business performance.

A new business model was expected by implementing ISO 27001 ISMS under the existing ISO 9001 QMS, and one of objectives is to identify the potential hazards by using a risk management process, InfoSec FMEA Circle, for developing a new business model "Virtual IP Chamber."

ICIP work group staff attended all scheduled training courses indicated in Step 14 before implementation of the QISM model. Those training courses included ISMS awareness and implementation, risk assessment methods and FMEA tools, internal ISMS auditor and ISMS lead auditor, etc. After those training were completed, we needed to prepare the core element in ISMS. That is Risk Assessment using InfoSec FMEA Circle.

During risk assessment evaluation process, we held 7 full days meeting to discuss different aspects of the information security flow in which all members in ICIP work group participated in. The most important evaluation conducted in the first meeting is to identify the information asset. Then, we created the Information Asset Evaluation summary table which linked the information asset into each processes under risk assessment. After that, we evaluated 133 control objectives given in the Annex of ISO 27001 and different work flows in our operation. Those work flows included ICDC customer order booking, Troubleshoot of the external tenant connected fiber, IPSC customer order booking, IP hardening/integration project process, multi-project wafer (MPW) shuttle and low-volume production (LVP) service, etc. Totally, 237 control objectives were evaluated and the RPNs were calculated. After going through the whole exercise, 18 critical points were identified and measures to mitigate the risks were shown in a RTP (see Table 5 InfoSec FMEA Circle results in ICDC and IPSC (sample)).

QISM implementation would be performed based on the outcome of risk assessment. The Information Asset Evaluation Form and Information Security FMEA Form are live documents which need to be updated if there are any changes in the process. RTP should be implemented accordingly in order to reduce the risk level of centre's operation. Apart from that, ISMS supplementary quality manual should be modified based on the risk assessment, identified work instructions for control objectives should be developed and documented. Business continuity plan should also be developed and documented, as well as drill test for DR site. After consolidating all control objectives and its measures, the Statement of Applicability (SOA) was developed and documented. SOA is like a content of a book and it is one of the most important documents for ISO 27001 certification. Based on our existing ISO 9001 document control, all ISMS documentation would be updated into electronic document management system (eDMS).

Table 5. InfoSec FMEA Circle results in ICDC and IPSC (sample)

Doc code	Process description	RTP identified	RPN (>100)	Remark
001	ISO27001 Control Objective A.5 to A.15	- Classification guidelines (7.2.1) - Routers and Switches Configuration - Router Administration - PIX Firewall Rules - User authentication for external connections (11.4.2) - Audit logging (10.10.1) - Monitoring system use (10.10.2) - Protection of log information (10.10.3) - Administrator and operator logs (10.10.4) - Fault logging (10.10.5)	224 200 200 200 160 140 140 140 140 140	All items score higher than 100 were identified for risk treatment plan (RTP).
002	ICDC order booking work flow FMEA	- Approve customer a/c and chase back credit information from customer, pass copy of approved Registration Form to ICDC	72	The risk is below 100, meaning that risk is acceptable after evaluation.
003	General IP Hardening / Integration Project	- Design environment is monitored by NOC	64	Same as Doc code 002
004	Troubleshoot of the External Tenant Connected Fiber through JLL	- Verify the status of External ICDC tenant Fiber port assignment	12	Same as Doc code 002
005	IP Servicing Centre, Customer Order Booking Work Flow	- Already set up procedure from CDN & 2-level password protection	45	Same as Doc code 002
006	Multi Project Wafer Shuttle and Low Volume Production Services Workflow	- Firewall / protection software is utilize inside the data centre	72	Same as Doc code 002
007	IC Design Centre, Network Equipment Change	- Automatic definition update from the internet	81	Same as Doc code 002
008	Virtual IP Chamber Work Flow	- Cross-check between engineer (i.e. email cc to another engineer in ICDC)	72	Same as Doc code 002

FMEA: failure mode and effects analysis, RTP: risk treatment plan, RPN: risk priority number.

6. CONCLUSION AND FUTURE WORK

After reviewing different risk management approaches and tools, as well as experts' experience in risk assessment, FMEA has been selected for developing a risk assessment tool for information security because of the semi-quantitative approach in calculating RPN. The IC Design Centre (ICDC) under Technology Support Centre in HKSTP employed the InfoSec FMEA Circle, by which 133 controls and many internal processes in the centre had been evaluated. Ultimately, ICDC was granted ISO 27001 certification by Hong Kong Quality Assurance Agency (HKQAA) in February 2009. Therefore, this study concludes that the FMEA risk assessment tool is entirely appropriate for the assessment of information security and assisting the implementation of QISM under ISO 27001 and ISO 9001 framework. Since information security awareness is increasing recently, many different industries pay more attention on ISMS. This study tried to employ FMEA, which is very familiar in manufacturing and engineering industries (e.g., automotive industry using TS 16949), for ISMS so as to influence other industries and reduce the barrier for implementing and adopting ISO 27001.

The limitations of FMEA are identified as follows:

1) RPNs are not continuous and heavily distributed at the bottom of the scale from 1 to 1000, causing interpretation problems between different RPNs (Chin *et al.*, 2009).
2) Same magnitude of RPNs can be obtained from different combinations of occurrence (*O*), severity (*S*) and detection (*D*), in which their hidden risk implications may be totally different (Chin *et al.*, 2008; Wang *et al*., 2009);
3) Sensitivity to small changes means that a small change in one factor has a much larger effect when the other factors are larger compared with when they are small (e.g., RPN on 9×9×**3** = 243 and on 9×9×**4** = 324; RPN in 3×4×**3** = 36 and on 3×4×**4** = 48);
4) Inadequate scaling of the ratios on occurrence table is not proportional or linear;
5) Other important factors are ignored, such as economic aspects (von Ahsen, 2008; Chin *et al.*, 2009);
6) Risk evaluation using RPN cannot always be assessed by detection (*D*) (Segismundo and Miguel, 2008); and
7) No exact rule is given to determine the probability of occurrence (*O*) and detection (*D*) (Segismundo and Miguel, 2008).

Therefore, the development of "InfoSec FMEA Circle" can provide solutions to overcome the above insufficiencies of FMEA stated by different scholars (Chin *et al.*, 2008, 2009; Wang *et al*., 2009; von Ahsen, 2008; Segismundo and Miguel, 2008; BS EN 60812:2006):

1) The proposed FMEA-based risk assessment is to set the risk acceptable level below or at the score of 100 (that is 10% of total score upper limit of 1000). Even though RPN is heavily distributed at the bottom (say below 100), the information asset classification shall also be considered. If it is in Class A, more attention shall be given during system review.
2) Development of the evaluation method for Information Asset Classification based on confidentiality, integrity and availability, it is an indicator to prioritize the RPNs if duplicate RPNs were calculated.
3) Since the acceptable risk level was suggested to be set at 100, the sensitivity of small change is not significant. Moreover, the information asset classification is added as an important indicator for further consideration.
4) The scaling system for evaluating of severity, occurrence and detection is from 1 to 10. Scale of each item was evaluated by group discussion in a focus group, based on internal experts' experience and past data. Therefore, it has overcome the inadequate scaling.
5) Economic aspect is out of scope in this study because the information security is the most critical aspect in IT business.
6) For information security, many monitoring and checking steps will be specified and performed automatically through the IT system. RPN is always assessed by "Detection."
7) Even if there is an absence of a standard guide to determine the probability of occurrence (*O*) and detection (*D*), the focus group interview can help to map out the definition of each score in occurrence (*O*) and detection (*D*).

ACKNOWLEDGMENTS

This research was supported by the SRG project of City UHK (No. 7002700).

REFERENCES

Baker, W. H. and Wallace, L. (2007), Is information security under control? Investigating quality in information security management, *IEEE Security and Privacy*, **5**(1), 36-44.

Barlette, Y. and Fomin, V. V. (2008), Exploring the suitability of IS security management standards for SMEs, *Proceedings of the 41st Hawaii International Conference on System Sciences*, Waikoloa, HI, 1-10.

Baskerville, R. (1991), Risk analysis: an interpretive feasibility tool in justifying information systems

security, *European Journal of Information Systems*, **1**(2), 121-130.

Brenner, J. (2007), ISO 27001: Risk management and compliance, *Risk Management*, **54**(1), 24-29.

British Standards Institution (2006), BS EN 60812:2006 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA).

British Standards Institution (2008), BS 31100:2008 Risk management - Code of practice.

British Standards Institution (2011), BS 31100:2011 Risk management - Code of practice and guidance for the implementation of BS ISO 31000.

Broderick, J. S. (2006), ISMS, security standards and security regulations, *Information Security Technical Report*, **11**(1), 26-31.

Chin, K. S., Chan, A., and Yang, J. B. (2008), Development of a fuzzy FMEA based product design system, *International Journal of Advanced Manufacturing Technology*, **36**(7-8), 633-649

Chin, K. S., Wang, Y. M., Poon, G. K. K., and Yang, J. B. (2009), Failure mode and effects analysis using a group-based evidential reasoning approach, *Computers and Operations Research*, **36**(6), 1768-1779.

Fomin, V. V., de Vries H. J., Barlette, Y., and Montpellier, F. (2008), ISO/IEC 27001 Information Systems Security Management Standard: exploring the reasons for low adoption, *Proceedings of the 3rd European Conference on Management of Technology*, Nice, France.

Fung, C. M. (2004), *The implementation procedures for information security management (access control) in BS 7799/ISO 17799*, M. S. Thesis, Department of Manufacturing Engineering and Engineering Management, City University of Hong Kong, China.

Halliday, S., Badenhorst, K., and Von Solms, R. (1996), A business approach to effective information technology risk analysis and management, *Information Management and Computer Security*, **4**(1), 19-31.

Humphreys, E. (2008), Information security management standards: compliance, governance and risk management, *Information Security Technical Report*, **13**(4), 247-255.

Institute of Risk Management (2002), *A Risk Management Standard*, Institute of Risk Management, London.

International Organization for Standardization (2000), ISO/IEC 17799:2000 Information technology - Code of practice for information security management.

International Organization for Standardization (2002), ISO/IEC Guide 73:2002 Risk management - Vocabulary - Guidelines for use in standards.

International Organization for Standardization (2005), ISO/IEC 27001:2005, Information technology - Security techniques - Information security management system–Requirements.

International Organization for Standardization (2009), ISO 31000:2009, Risk management - Principles and guidelines.

International Organization for Standardization (2011), ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management.

Kwok, L. F. and Longley, D. (1999), Information security management and modeling, *Information Management and Computer Security*, **7**(1), 30-39.

Lai, L. K. H., Chin, K. S., and Tsang, A. H. C. (2010), Risk management of information security: information security FMEA circle, *Proceedings of the 8th Asia Network for Quality (ANQ) Congress*, New Delhi, India, paper HK01.

Misra, S. C., Kumar, V., and Kumar, U. (2007), A strategic modeling technique for information security risk assessment, *Information Management and Computer Security*, **15**(1), 64-77.

Segismundo, A. and Miguel P. A. C. (2008), Failure mode and effects analysis (FMEA) in the context of risk management in new product development: a case study in an automotive company, *International Journal of Quality and Reliability Management*, **25**(9), 899-912.

Spinellis, D., Kokolakis, S., and Gritzalis, S. (1999), Security requirements, risks and recommendations for small enterprise and home-office environments, *Information Management and Computer Security*, **7**(3), 121-128.

Standards Association of Australia (1999), AS/NZS 4360: 1999 Risk management.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. (2006), Formulating information systems risk management strategies through cultural theory, *Information Management and Computer Security*, **14**(3), 198-217.

von Ahsen, A. (2008), Cost-oriented failure mode and effects analysis, *International Journal of Quality and Reliability Management*, **25**(5), 466-476.

Wang, Y. M., Chin, K. S., Poon, G. K. K., and Yang, J. B. (2009), Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean, *Expert Systems with Applications*, **36**(2), 1195-1207.