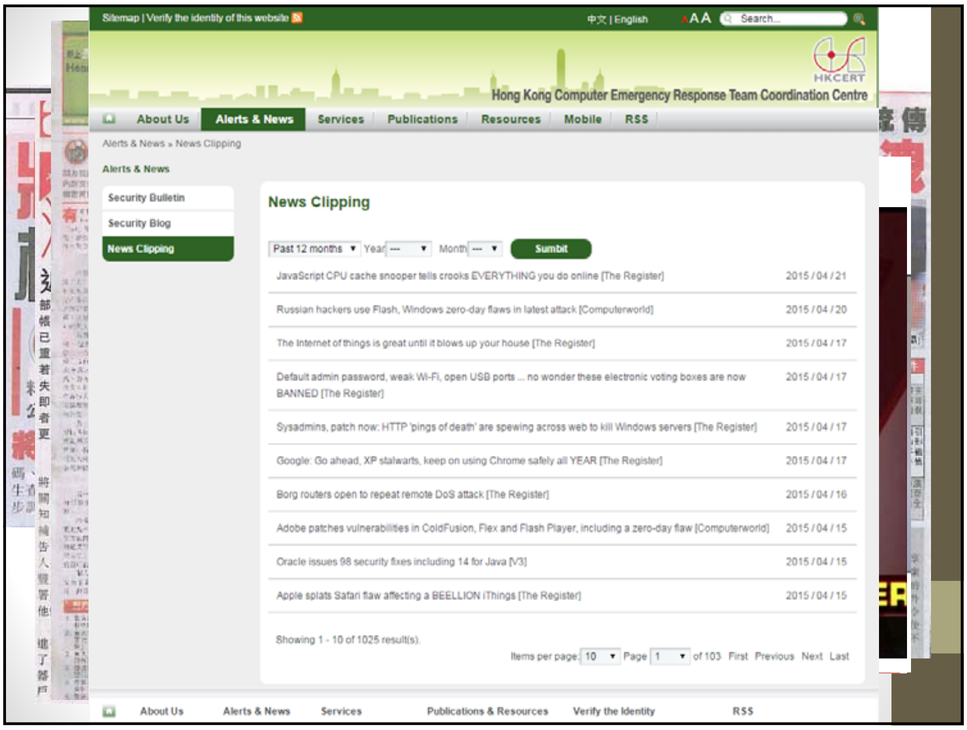
# QMS Based Information Security Management System – Case Study

HKSTP

**Lotto Lai**
**Manager, Quality System**
June 19, 2015

## Content

- IT Environment in HK (Since 2008)
- ISO Certificates in the World
- What is Information Security Management System? (ISO 27001)
- What is Quality Management System? (ISO 9001)
- QMS based Information Management System (QISM) model development
- Information Security FMEA
- HKSTP Case
- Create Value in ICDC & IPSC Business – ISO 27001 certified Secure Virtual IP Chamber (SVIPC)
- Conclusion



News Clipping

| | |
|---|---|
| JavaScript CPU cache snooper tells crooks EVERYTHING you do online [The Register] | 2015 / 04 / 21 |
| Russian hackers use Flash, Windows zero-day flaws in latest attack [Computerworld] | 2015 / 04 / 20 |
| The Internet of things is great until it blows up your house [The Register] | 2015 / 04 / 17 |
| Default admin password, weak Wi-Fi, open USB ports ... no wonder these electronic voting boxes are now BANNED [The Register] | 2015 / 04 / 17 |
| Sysadmins, patch now: HTTP 'pings of death' are spewing across web to kill Windows servers [The Register] | 2015 / 04 / 17 |
| Google: Go ahead, XP stalwarts, keep on using Chrome safely all YEAR [The Register] | 2015 / 04 / 17 |
| Borg routers open to repeat remote DoS attack [The Register] | 2015 / 04 / 16 |
| Adobe patches vulnerabilities in ColdFusion, Flex and Flash Player, including a zero-day flaw [Computerworld] | 2015 / 04 / 15 |
| Oracle issues 98 security fixes including 14 for Java [V3] | 2015 / 04 / 15 |
| Apple splats Safari flaw affecting a BEELLION iThings [The Register] | 2015 / 04 / 15 |

Showing 1 - 10 of 1025 result(s).

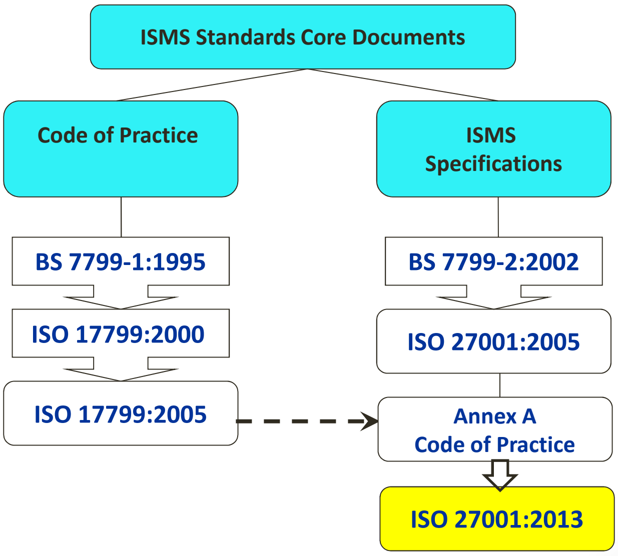
# What is Information Security Management System (ISMS)?

- **Information** is an asset that, like other important business assets, ***is essential to an organization's business*** and consequently needs to be ***suitably protected***.

- **Information Security** means preservation of ***confidentiality, integrity and availability*** of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved;

- **Information Security Management System** is a part of the overall management system, based on a ***business risk approach***, to establish, implement, operate, monitor, review, maintain and improve information security.

# Backgrounds



ISMS Standards Core Documents

Code of Practice

ISMS Specifications

BS 7799-1:1995

ISO 17799:2000

ISO 17799:2005

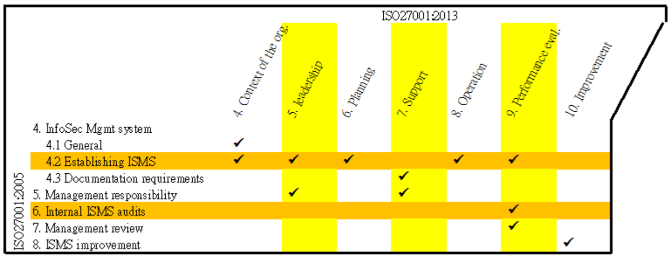
BS 7799-2:2002

ISO 27001:2005

Annex A Code of Practice

ISO 27001:2013

# ISO 27001:2005 vs 2013



| ISO27001:2005 \ ISO27001:2013 | 4. Context of the org. | 5. leadership | 6. Planning | 7. Support | 8. Operation | 9. Performance eval. | 10. Improvement |
|---|---|---|---|---|---|---|---|
| 4. InfoSec Mgmt system | | | | | | | |
| 4.1 General | ✓ | | | | | | |
| 4.2 Establishing ISMS | ✓ | ✓ | ✓ | | ✓ | ✓ | |
| 4.3 Documentation requirements | | | | ✓ | | | |
| 5. Management responsibility | | ✓ | | ✓ | | | |
| 6. Internal ISMS audits | | | | | | ✓ | |
| 7. Management review | | | | | | ✓ | |
| 8. ISMS improvement | | | | | | | ✓ |

| 2005 Version | 2013 Version |
|---|---|
| Number of sections in Annex A<br>**11** | Number of sections in Annex A<br>**14** |
| Number of controls in Annex A<br>**133** | Number of controls in Annex A<br>**114** |

# Annex A: Control Objectives and Controls

**Policy**

A.5 InfoSec Policies

A.6 Org InfoSec

A.8 Asset Management

**Organization Structure**

A.7 HR Security

A.9 Access Control

**Process & Procedure**

A.10. Cryptography

A.12 Operation Security

A.13 Communication Security

A.14 System acquisition, develop & Maint

**Hardware**

A.11 Physical & Environmental Security

A.15 Supplier relationship

**Software**

A.16 InfoSec Incident Mgmt.

A.17 BCM

# What is Quality Management System (QMS)?

**Based on ISO9000:2005 definition:**

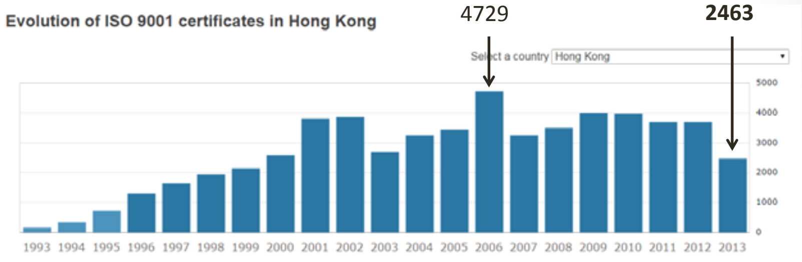
- **Quality** means degree to which a set of inherent characteristics fulfils requirements;
- **Management** means coordinated activities to direct and control an organization;
- **System** means a set of interrelated or interacting elements; and so
- **Quality Management System** is a management system to direct and control an organization with regard to quality.

# ISO 27001 in the World

| Top 10 Countries for ISO/IEC 27001 Certificates - 2013 | | |
|---|---|---|
| 1 | Japan | 7084 |
| 2 | India | 1931 |
| 3 | United Kingdom | 1923 |
| 4 | China | 1710 |
| 5 | Italy | 901 |
| 6 | Taipei, Chinese | 861 |
| 7 | Romania | 840 |
| 8 | Spain | 799 |
| 9 | Germany | 581 |
| 10 | USA | 566 |

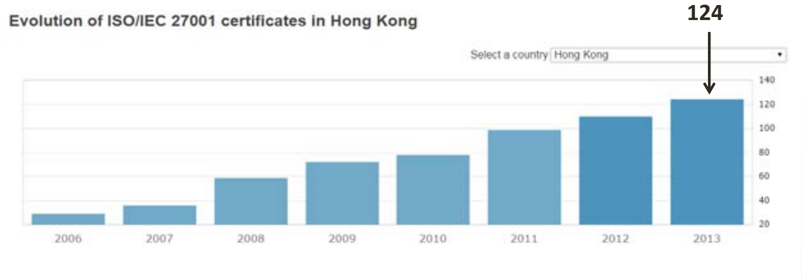
| China | 1710 |
|---|---|
| Hong Kong, China | 124 |
| Macau, China | 15 |
| Taipei, Chinese | 861 |

# ISO 9001 and ISO 27001 in HK

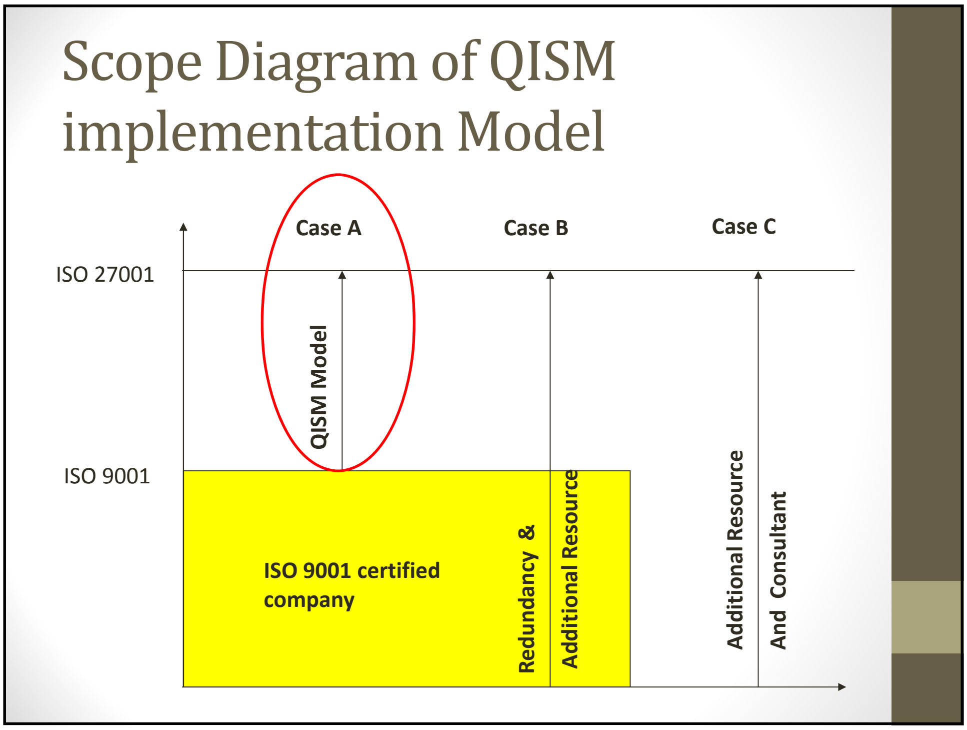

Evolution of ISO 9001 certificates in Hong Kong

4729

2463


Evolution of ISO/IEC 27001 certificates in Hong Kong

124



# Scope Diagram of QISM implementation Model

Case A

Case B

Case C

ISO 27001

ISO 9001

QISM Model

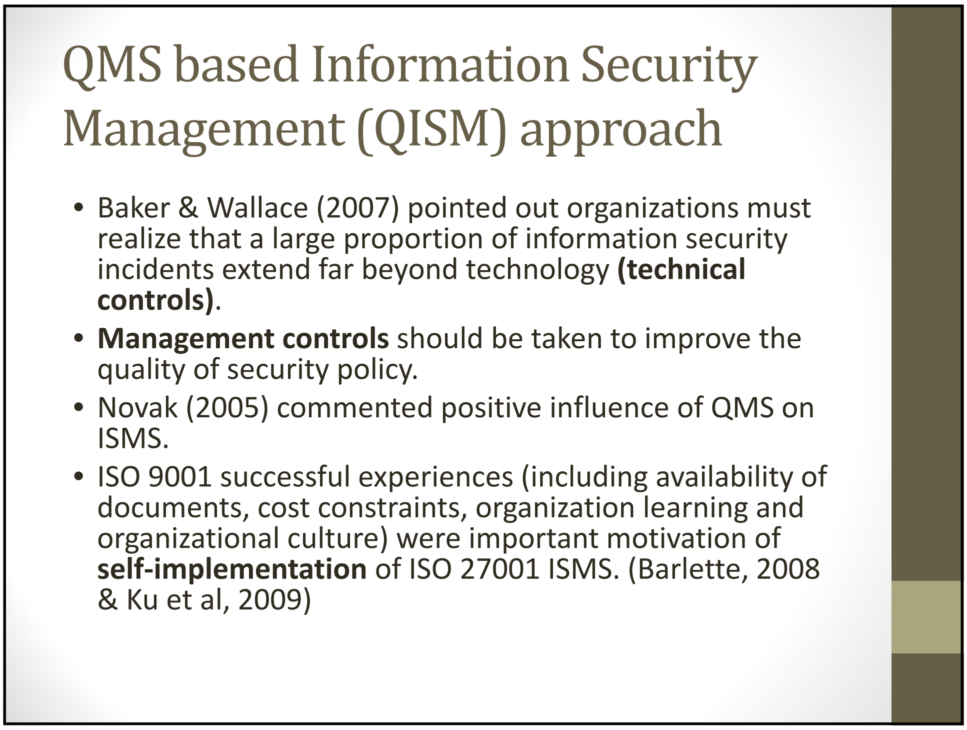
ISO 9001 certified company

Redundancy &

Additional Resource

Additional Resource

And Consultant

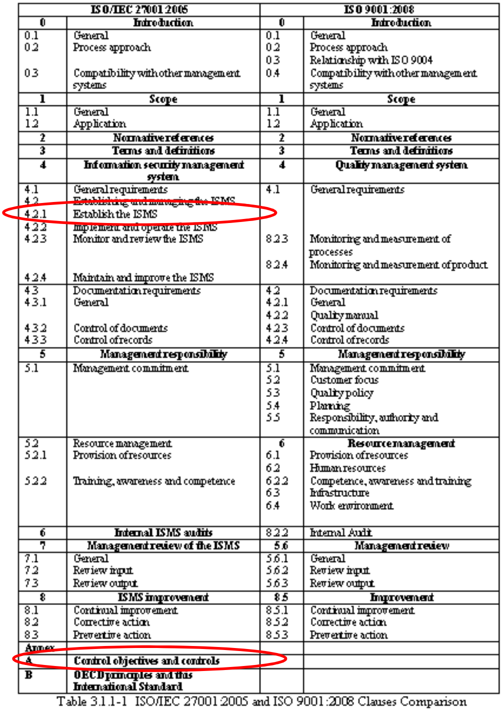


# QMS based Information Security Management (QISM) approach

- Baker & Wallace (2007) pointed out organizations must realize that a large proportion of information security incidents extend far beyond technology **(technical controls)**.
- **Management controls** should be taken to improve the quality of security policy.
- Novak (2005) commented positive influence of QMS on ISMS.
- ISO 9001 successful experiences (including availability of documents, cost constraints, organization learning and organizational culture) were important motivation of **self-implementation** of ISO 27001 ISMS. (Barlette, 2008 & Ku et al, 2009)

# Comparison of ISO 9001 and ISO 27001

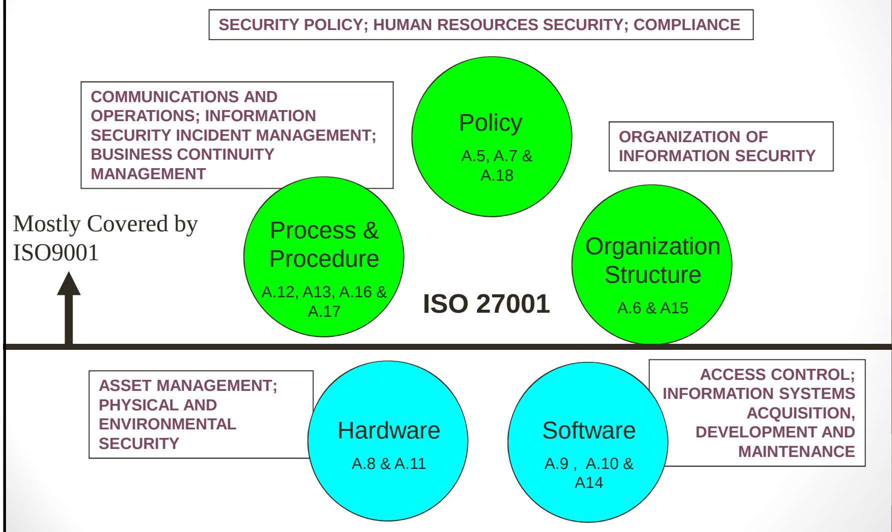
- About 90% of the management system requirements are found to be compatible with each other.
- The two major differences between ISO 27001 and ISO 9001 are shown as follows.
  - risk assessment methodology in Clause 4.2.1
  - "Annex A – Control Objectives and Controls": 133 Controls are specified.



| ISO/IEC 27001:2005 | | ISO 9001:2008 | |
|---|---|---|---|
| **0** | **Introduction** | **0** | **Introduction** |
| 0.1 | General | 0.1 | General |
| 0.2 | Process approach | 0.2 | Process approach |
| | | 0.3 | Relationship with ISO 9004 |
| 0.3 | Compatibility with other management systems | 0.4 | Compatibility with other management systems |
| **1** | **Scope** | **1** | **Scope** |
| 1.1 | General | 1.1 | General |
| 1.2 | Application | 1.2 | Application |
| **2** | **Normative references** | **2** | **Normative references** |
| **3** | **Terms and definitions** | **3** | **Terms and definitions** |
| **4** | **Information security management system** | **4** | **Quality management system** |
| 4.1 | General requirements | 4.1 | General requirements |
| 4.2 | Establishing and managing the ISMS | | |
| 4.2.1 | Establish the ISMS | | |
| 4.2.2 | Implement and operate the ISMS | | |
| 4.2.3 | Monitor and review the ISMS | 8.2.3 | Monitoring and measurement of processes |
| | | 8.2.4 | Monitoring and measurement of product |
| 4.2.4 | Maintain and improve the ISMS | | |
| 4.3 | Documentation requirements | 4.2 | Documentation requirements |
| 4.3.1 | General | 4.2.1 | General |
| | | 4.2.2 | Quality manual |
| 4.3.2 | Control of documents | 4.2.3 | Control of documents |
| 4.3.3 | Control of records | 4.2.4 | Control of records |
| **5** | **Management responsibility** | **5** | **Management responsibility** |
| 5.1 | Management commitment | 5.1 | Management commitment |
| | | 5.2 | Customer focus |
| | | 5.3 | Quality policy |
| | | 5.4 | Planning |
| | | 5.5 | Responsibility, authority and communication |
| 5.2 | Resource management | **6** | **Resource management** |
| 5.2.1 | Provision of resources | 6.1 | Provision of resources |
| | | 6.2 | Human resources |
| 5.2.2 | Training, awareness and competence | 6.2.2 | Competence, awareness and training |
| | | 6.3 | Infrastructure |
| | | 6.4 | Work environment |
| **6** | **Internal ISMS audits** | 8.2.2 | Internal Audit |
| **7** | **Management review of the ISMS** | **5.6** | **Management review** |
| 7.1 | General | 5.6.1 | General |
| 7.2 | Review input | 5.6.2 | Review input |
| 7.3 | Review output | 5.6.3 | Review output |
| **8** | **ISMS improvement** | **8.5** | **Improvement** |
| 8.1 | Continual improvement | 8.5.1 | Continual improvement |
| 8.2 | Corrective action | 8.5.2 | Corrective action |
| 8.3 | Preventive action | 8.5.3 | Preventive action |
| **Annex** | | | |
| **A** | **Control objectives and controls** | | |
| **B** | **OECD principles and this International Standard** | | |

Table 3.1.1-1 ISO/IEC 27001:2005 and ISO 9001:2008 Clauses Comparison

# Five Control Objective Group

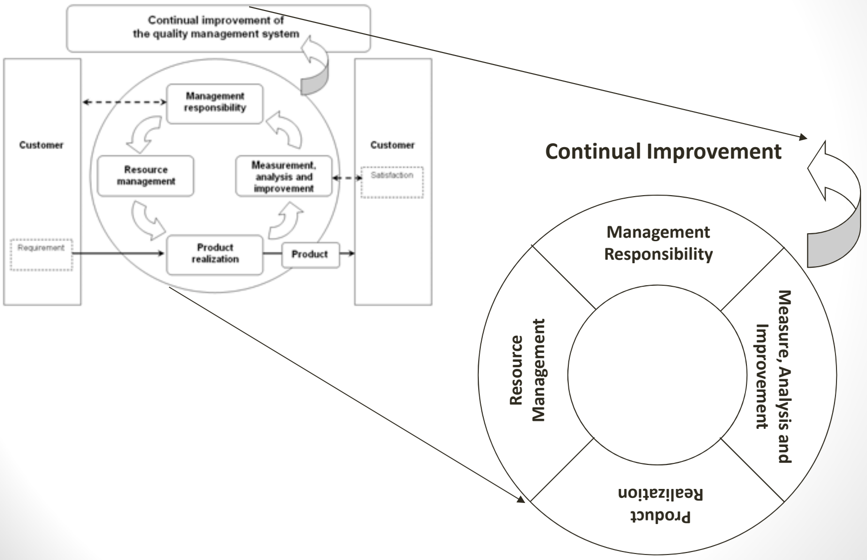

SECURITY POLICY; HUMAN RESOURCES SECURITY; COMPLIANCE
COMMUNICATIONS AND OPERATIONS; INFORMATION SECURITY INCIDENT MANAGEMENT; BUSINESS CONTINUITY MANAGEMENT
Policy
A.5, A.7 & A.18
ORGANIZATION OF INFORMATION SECURITY
Mostly Covered by ISO9001
Process & Procedure
A.12, A13, A.16 & A.17
ISO 27001
Organization Structure
A.6 & A15
ASSET MANAGEMENT; PHYSICAL AND ENVIRONMENTAL SECURITY
Hardware
A.8 & A.11
Software
A.9 , A.10 & A14
ACCESS CONTROL; INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

# QISM Implementation Model Development

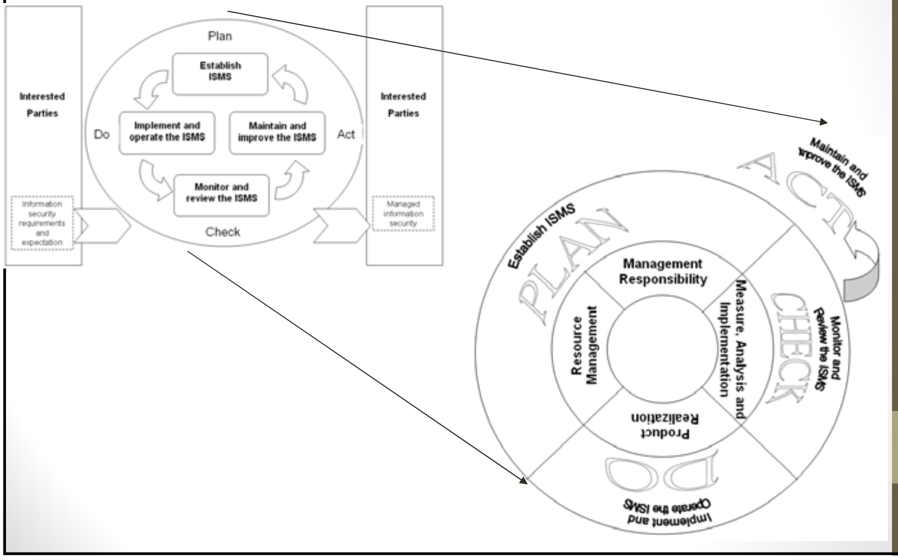
- The first objective of this study aims to develop QMS based Information Security Management (QISM) Model for assisting ISO 9001 certified companies to implement ISO 27001 ISMS.

- Development of the QISM model is divided into 4 steps
  - Step 1: Review quality management system model and extract the core elements
  - Step 2: Review information security management system model and combine its core elements with those in the QMS model
  - Step 3: Review security element relationships (SER) model and develop conceptual security model framework
  - Step 4: Combine all elements to form QISM model

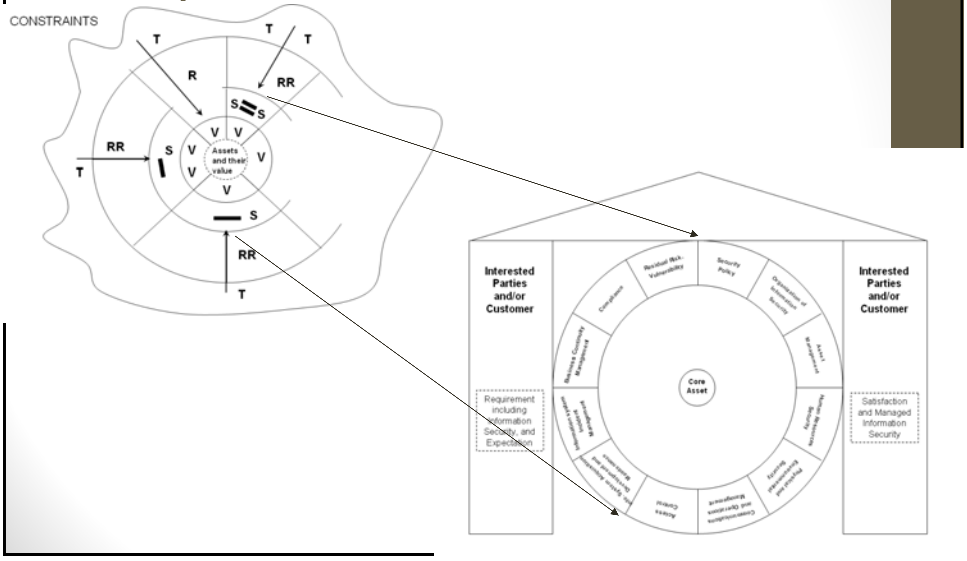
## Step 1: Review Quality Management System Model Extract the Core Elements


Continual improvement of the quality management system
Customer
Management responsibility
Resource management
Measurement, analysis and improvement
Satisfaction
Requirement
Product realization
Product
Customer
Continual Improvement
Management Responsibility
Resource Management
Measure, Analysis and Improvement
Product Realization

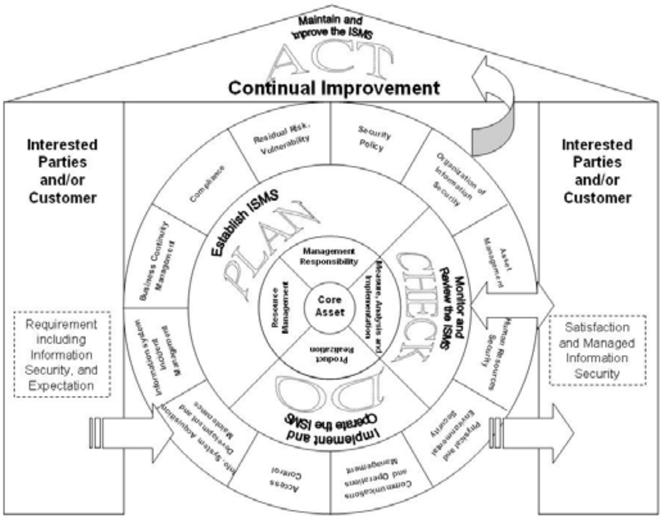
## Step 2: Review ISMS Model & Combine its Core Elements with those in the QMS Model


Interested Parties
Information security requirements and expectation
Plan
Establish ISMS
Implement and operate the ISMS
Maintain and improve the ISMS
Monitor and review the ISMS
Do
Act
Check
Interested Parties
Managed information security
Establish ISMS
PLAN
ACT
Maintain and improve the ISMS
Management Responsibility
Resource Management
Measure, Analysis and Implementation
CHECK
Monitor and Review the ISMS
Product Realization
DO
Implement and Operate the ISMS

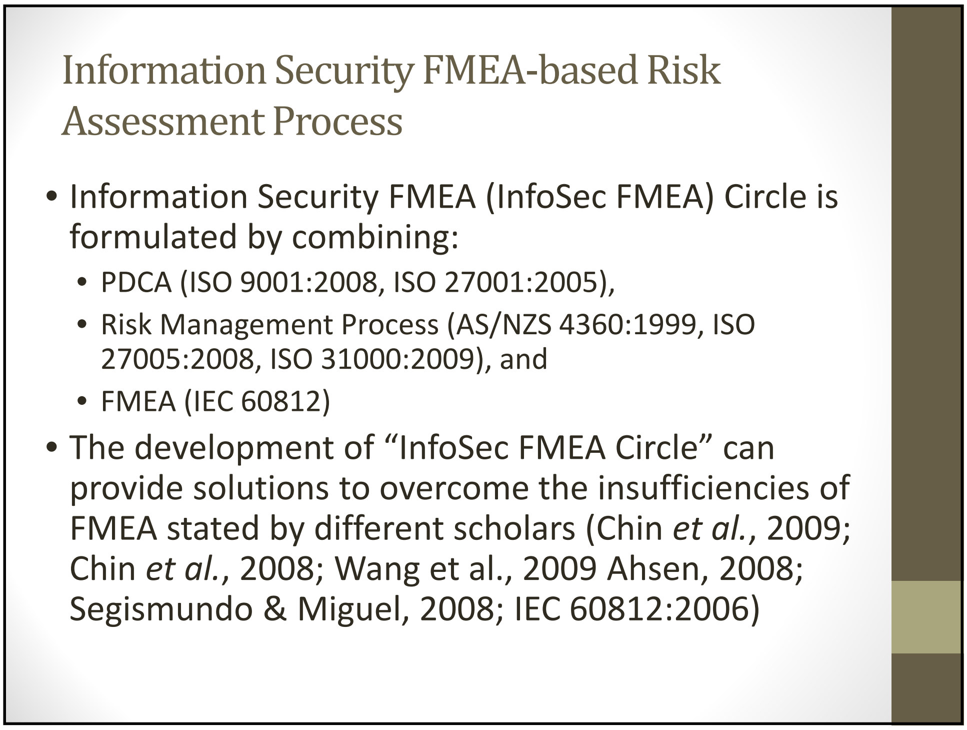
## Step 3: Review Security Element Relationships Model & Develop Conceptual Security Model Framework


CONSTRAINTS
T
T
T
T
T
R
RR
RR
RR
S
S
S
S
V
V
V
V
V
V
Assets and their value
Interested Parties and/or Customer
Requirement including Information Security, and Expectation
Residual Risk, Vulnerability
Security Policy
Organization of Information Security
Asset Management
Human Resources Security
Physical and Environmental Security
Communications and Operations Management
Access Control
Info. System Acquisition, Development and Maintenance
Information Security Incident Management
Business Continuity Management
Compliance
Core Asset
Interested Parties and/or Customer
Satisfaction and Managed Information Security

## Step 4: Combine all Elements to form QISM Model

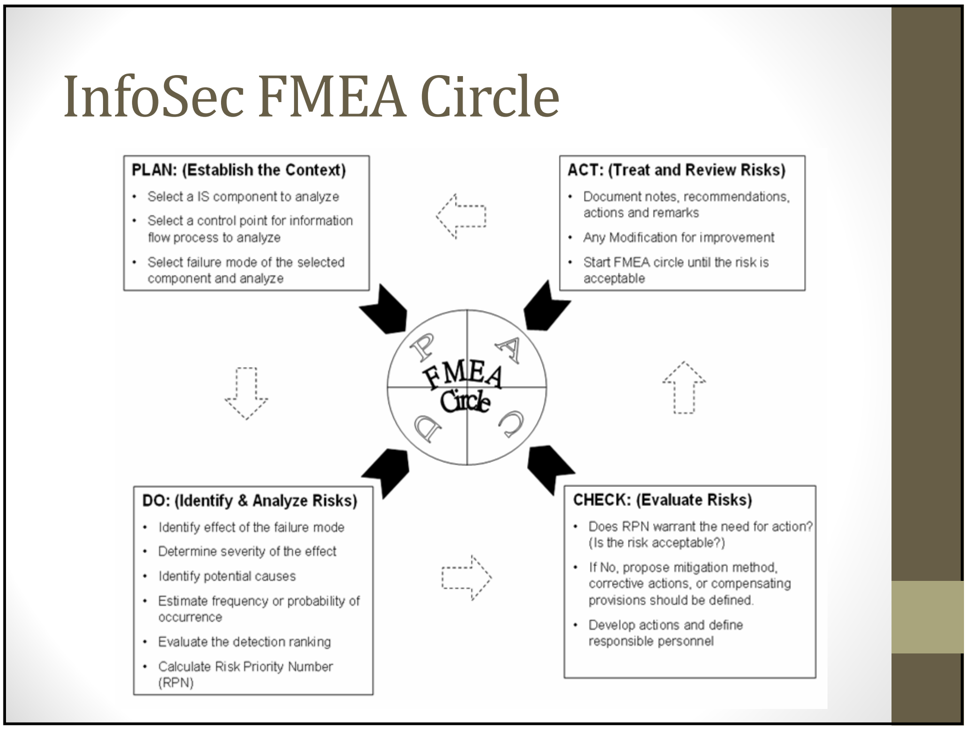

Maintain and improve the ISMS
ACT
Continual Improvement
Interested Parties and/or Customer
Interested Parties and/or Customer
Residual Risk, Vulnerability
Security Policy
Organization of Information Security
Asset Management
Human Resources Security
Physical and Environmental Security
Communications and Operations Management
Access Control
Info. System Acquisition Development and Maintenance
Information Security Incident Management
Business Continuity Management
Compliance
Establish ISMS
PLAN
Monitor and Review the ISMS
CHECK
Implement and Operate the ISMS
DO
Management Responsibility
Measure, Analysis and Implementation
Product Realization
Resource Management
Core Asset
Requirement including Information Security, and Expectation
Satisfaction and Managed Information Security

## InfoSec Risk Assessment



## Information Security FMEA-based Risk Assessment Process

- Information Security FMEA (InfoSec FMEA) Circle is formulated by combining:
  - PDCA (ISO 9001:2008, ISO 27001:2005),
  - Risk Management Process (AS/NZS 4360:1999, ISO 27005:2008, ISO 31000:2009), and
  - FMEA (IEC 60812)
- The development of “InfoSec FMEA Circle” can provide solutions to overcome the insufficiencies of FMEA stated by different scholars (Chin *et al.*, 2009; Chin *et al.*, 2008; Wang et al., 2009 Ahsen, 2008; Segismundo & Miguel, 2008; IEC 60812:2006)



## InfoSec FMEA Circle

**PLAN: (Establish the Context)**

- Select a IS component to analyze
- Select a control point for information flow process to analyze
- Select failure mode of the selected component and analyze

**ACT: (Treat and Review Risks)**

- Document notes, recommendations, actions and remarks
- Any Modification for improvement
- Start FMEA circle until the risk is acceptable

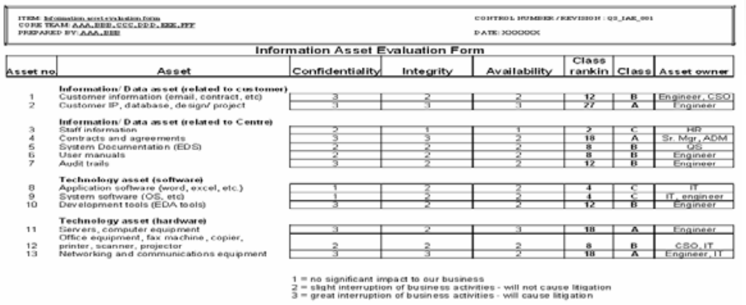
**DO: (Identify & Analyze Risks)**

- Identify effect of the failure mode
- Determine severity of the effect
- Identify potential causes
- Estimate frequency or probability of occurrence
- Evaluate the detection ranking
- Calculate Risk Priority Number (RPN)

**CHECK: (Evaluate Risks)**

- Does RPN warrant the need for action? (Is the risk acceptable?)
- If No, propose mitigation method, corrective actions, or compensating provisions should be defined.
- Develop actions and define responsible personnel

# Information Asset Evaluation



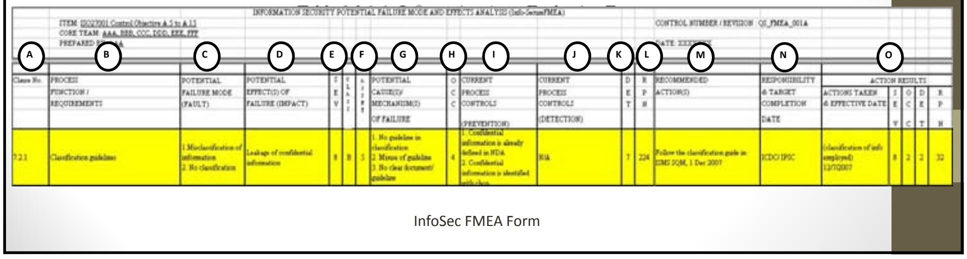
ITEM: Information asset evaluation form
CORE TEAM: AAA,BBB,CCC,DDD,EEE,FFF
PREPARED BY: AAA,BBB

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



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: XXXXXXX

| A | B | C | D | E | F | | G | H | I | J | K | L | M | N | O | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | ACTION RESULTS | | | | |
| Clause No. | PROCESS FUNCTION / REQUIREMENTS | POTENTIAL FAILURE MODE (FAULT) | POTENTIAL EFFECT(S) OF FAILURE (IMPACT) | SEV | CLASS | [illegible] | 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 DATE | SEV | OCC | DET | RPN |
| 7.2.1 | Classification guidelines | 1. Misclassification of information<br>2. No classification | Leakage of confidential information | 8 | B | 5 | 1. No guideline in classification<br>2. Misuse of guideline<br>3. No clear document/ guideline | 4 | 1. Confidential information is already defined in NDA<br>2. Confidential information is identified with class | N/A | 7 | 224 | Follow the classification guide in ISMS SQM, 1 Dec 2007 | ICDC/ IPSC | (classification of info employed) 12/?/2007 | 8 | 2 | 2 | 32 |

InfoSec FMEA Form

# Calculation of Risk Priority Number (RPN)

- Risk Priority Number (RPN) is the product of Severity (S), Occurrence (O) and Detection (D) rankings (See Table 3.2.1-2 – Item L).
- RPN = Severity (S) x Occurrence (O) x Detectability (D) …………….(Eq.1)
- RPN is calculated for each potential failure mode and the most important failure mode with the highest RPN number can be subsequently found.

## Implementation of InfoSec FMEA circle

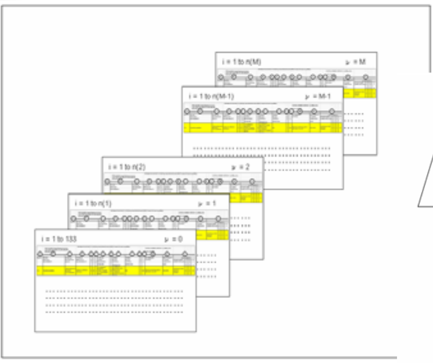

i = 1 to n(M)
μ = M
i = 1 to n(M-1)
μ = M-1
i = 1 to n(2)
μ = 2
i = 1 to n(1)
μ = 1
i = 1 to 133
μ = 0

Figure 3.2.2-1 Info-Secure FMEA Forms after M cycle

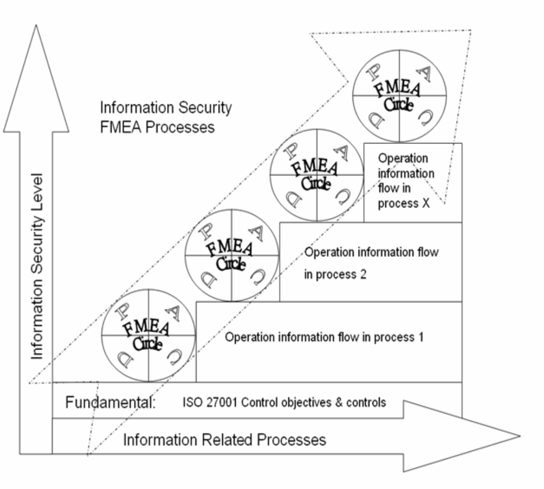
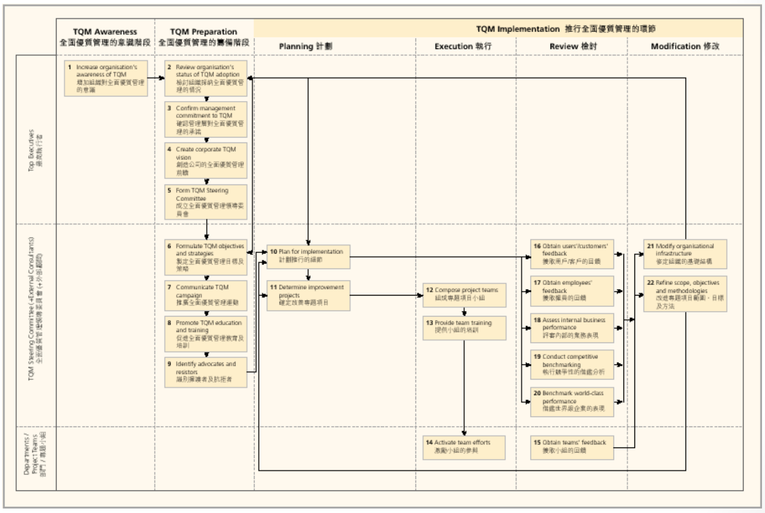

Information Security Level
Information Security
FMEA Processes
P
A
FMEA
Circle
D
C
Operation information flow in process X
Operation information flow in process 2
Operation information flow in process 1
Fundamental:
ISO 27001 Control objectives & controls
Information Related Processes

Figure 3.2.2-2 Info-Secure FMEA Circle Implementation

## QISM Implementation Roadmap

- QISM Implementation Roadmap is an implementation guideline for ISO 9001 certified companies to implement ISO 27001 management systems.
- 24-step guideline was developed to facilitate QMS based Information Security Management (QISM) adoption through the Awareness-Preparation-Implementation phases.

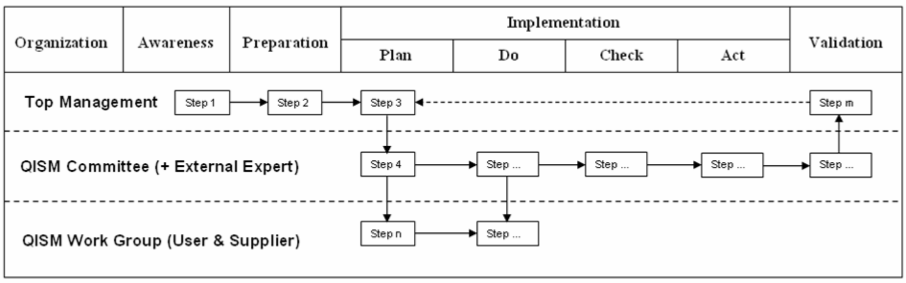
# Reference to TQM Roadmap

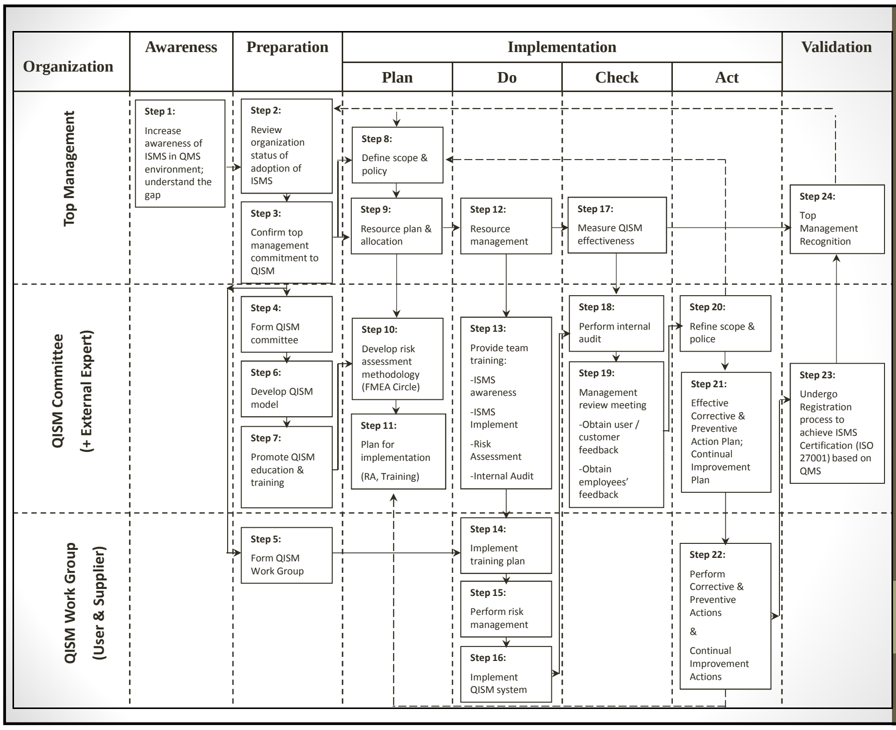

TQM Awareness
全面優質管理的意識階段
TQM Preparation
全面優質管理的籌備階段
TQM Implementation 推行全面優質管理的環節
Planning 計劃
Execution 執行
Review 檢討
Modification 修改
Top Executives
最高執行者
TQM Steering Committee (+External Consultants)
全面優質管理領導委員會 (+外部顧問)
Departments / Project Teams
部門 / 專題小組
1 Increase organisation's awareness of TQM
增加組織對全面優質管理的意識
2 Review organisation's status of TQM adoption
檢討組織採納全面優質管理的情況
3 Confirm management commitment to TQM
確認管理層對全面優質管理的承諾
4 Create corporate TQM vision
創造公司的全面優質管理前瞻
5 Form TQM Steering Committee
成立全面優質管理領導委員會
6 Formulate TQM objectives and strategies
製定全面優質管理目標及策略
7 Communicate TQM campaign
推廣全面優質管理運動
8 Promote TQM education and training
促進全面優質管理教育及培訓
9 Identify advocates and resistors
識別擁護者及抗拒者
10 Plan for implementation
計劃推行的細節
11 Determine improvement projects
確定改善專題項目
12 Compose project teams
組成專題項目小組
13 Provide team training
提供小組的培訓
14 Activate team efforts
激勵小組的參與
15 Obtain teams' feedback
獲取小組的回饋
16 Obtain users'/customers' feedback
獲取用戶/客戶的回饋
17 Obtain employees' feedback
獲取僱員的回饋
18 Assess internal business performance
評審內部的業務表現
19 Conduct competitive benchmarking
執行競爭性的借鑑分析
20 Benchmark world-class performance
借鑑世界級企業的表現
21 Modify organisational infrastructure
修定組織的基礎結構
22 Refine scope, objectives and methodologies
改進專題項目範圍、目標及方法

(Source:Chin & Dale, 2001)

# A 24-step Implementation Guideline of QISM Roadmap

- Throughout the execution of QISM implementation roadmap, top management, QISM committee members, work group members, users, suppliers, as well as external experts, as appropriate, were involved.





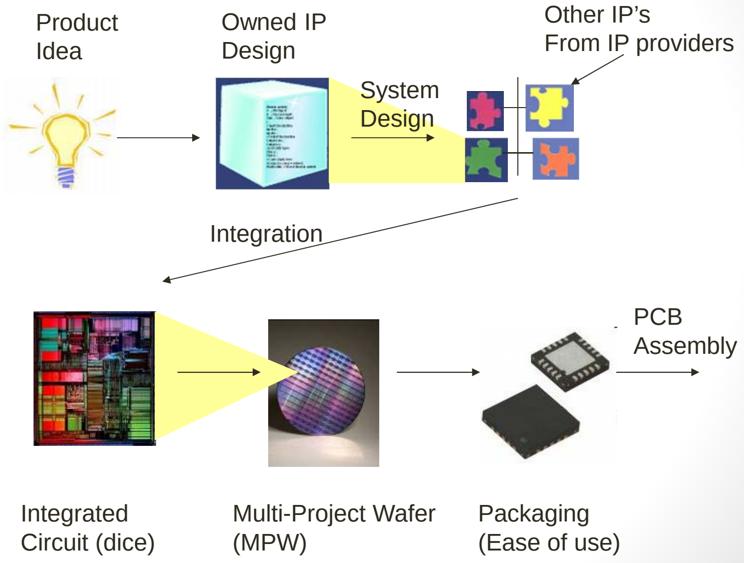
| Organization | Awareness | Preparation | Implementation | | | | Validation |
|---|---|---|---|---|---|---|---|
| | | | Plan | Do | Check | Act | |
| Top Management | **Step 1:** Increase awareness of ISMS in QMS environment; understand the gap | **Step 2:** Review organization status of adoption of ISMS<br>**Step 3:** Confirm top management commitment to QISM | **Step 8:** Define scope & policy<br>**Step 9:** Resource plan & allocation | **Step 12:** Resource management | **Step 17:** Measure QISM effectiveness | | **Step 24:** Top Management Recognition |
| QISM Committee (+ External Expert) | | **Step 4:** Form QISM committee<br>**Step 6:** Develop QISM model<br>**Step 7:** Promote QISM education & training | **Step 10:** Develop risk assessment methodology (FMEA Circle)<br>**Step 11:** Plan for implementation (RA, Training) | **Step 13:** Provide team training: -ISMS awareness -ISMS Implement -Risk Assessment -Internal Audit | **Step 18:** Perform internal audit<br>**Step 19:** Management review meeting -Obtain user / customer feedback -Obtain employees' feedback | **Step 20:** Refine scope & police<br>**Step 21:** Effective Corrective & Preventive Action Plan; Continual Improvement Plan | **Step 23:** Undergo Registration process to achieve ISMS Certification (ISO 27001) based on QMS |
| QISM Work Group (User & Supplier) | | **Step 5:** Form QISM Work Group | | **Step 14:** Implement training plan<br>**Step 15:** Perform risk management<br>**Step 16:** Implement QISM system | | **Step 22:** Perform Corrective & Preventive Actions & Continual Improvement Actions | |

# HKSTP Case Study

# Introduction of ICDC & IPSC

- ICDC provides technical support and services on using the state-of-the-art IC design tools, including mixed mode, analogue, digital, and SOC to HKSTP's tenants and incubates.
- IPSC provides technical support to semiconductor IP and services including IP licensing, IP hardening, IP integration and IP verification, as well as, MPW & LVP to HKSTP's tenants and incubates.
- **Objectives**
  - To support IC development in a protected environment
  - The facilitate the use of and license of Silicon Intellectual Properties through the Centres

# Brief Introduction of Modern Integrated Circuit (IC) Design



Product Idea

Owned IP Design

System Design

Other IP's From IP providers

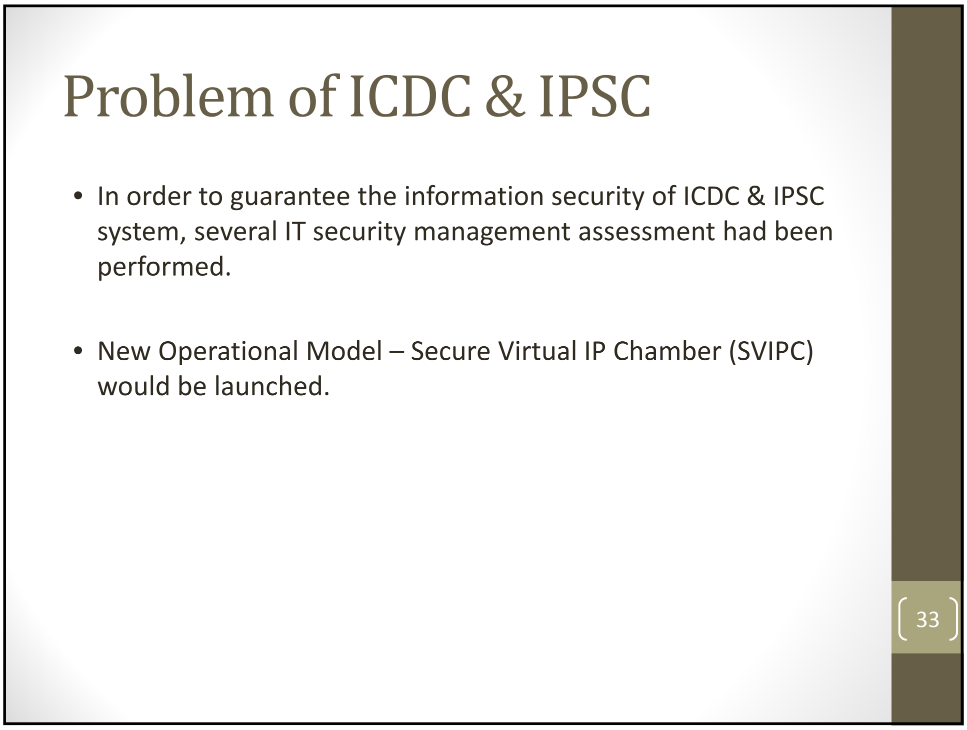
Integration

PCB Assembly

Integrated Circuit (dice)

Multi-Project Wafer (MPW)

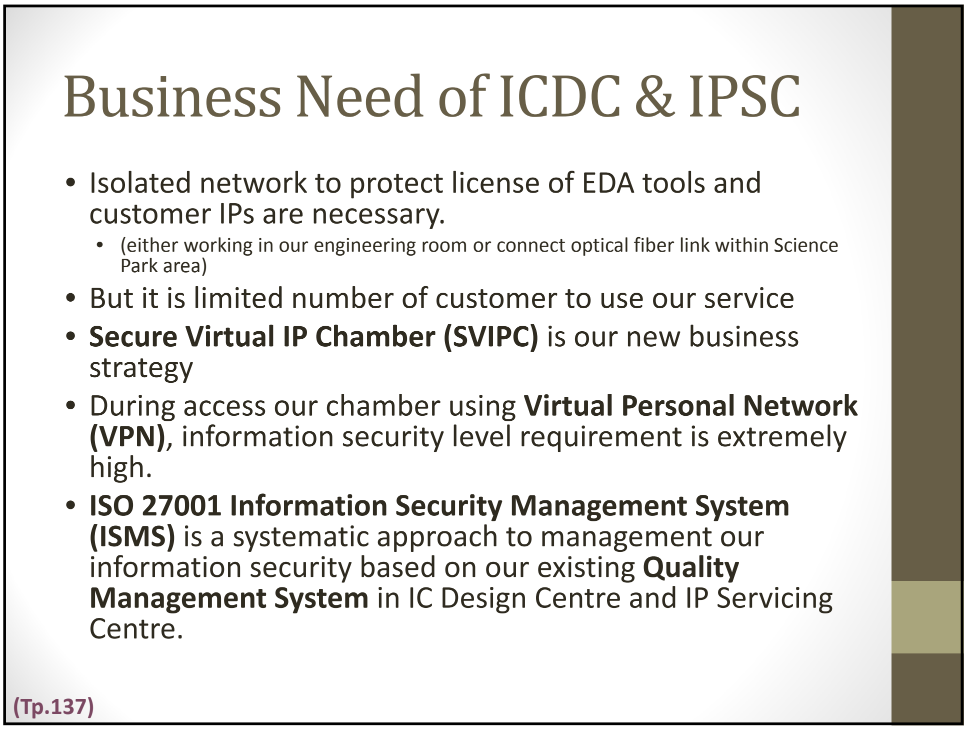
Packaging (Ease of use)



## Problem of ICDC & IPSC

- In order to guarantee the information security of ICDC & IPSC system, several IT security management assessment had been performed.
- New Operational Model – Secure Virtual IP Chamber (SVIPC) would be launched.

33

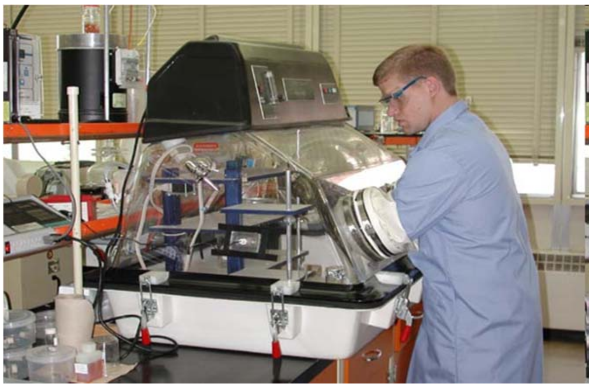


## Business Need of ICDC & IPSC

- Isolated network to protect license of EDA tools and customer IPs are necessary.
  - (either working in our engineering room or connect optical fiber link within Science Park area)
- But it is limited number of customer to use our service
- **Secure Virtual IP Chamber (SVIPC)** is our new business strategy
- During access our chamber using **Virtual Personal Network (VPN)**, information security level requirement is extremely high.
- **ISO 27001 Information Security Management System (ISMS)** is a systematic approach to management our information security based on our existing **Quality Management System** in IC Design Centre and IP Servicing Centre.

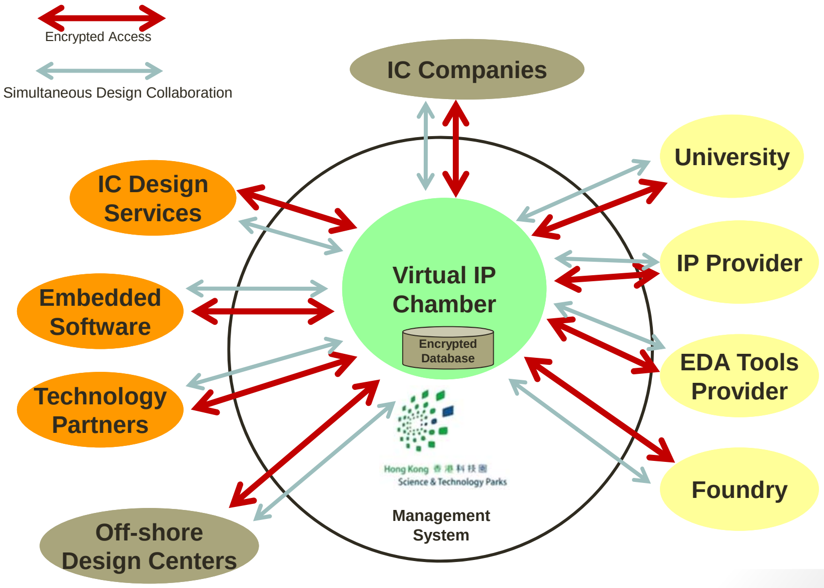
**(Tp.137)**

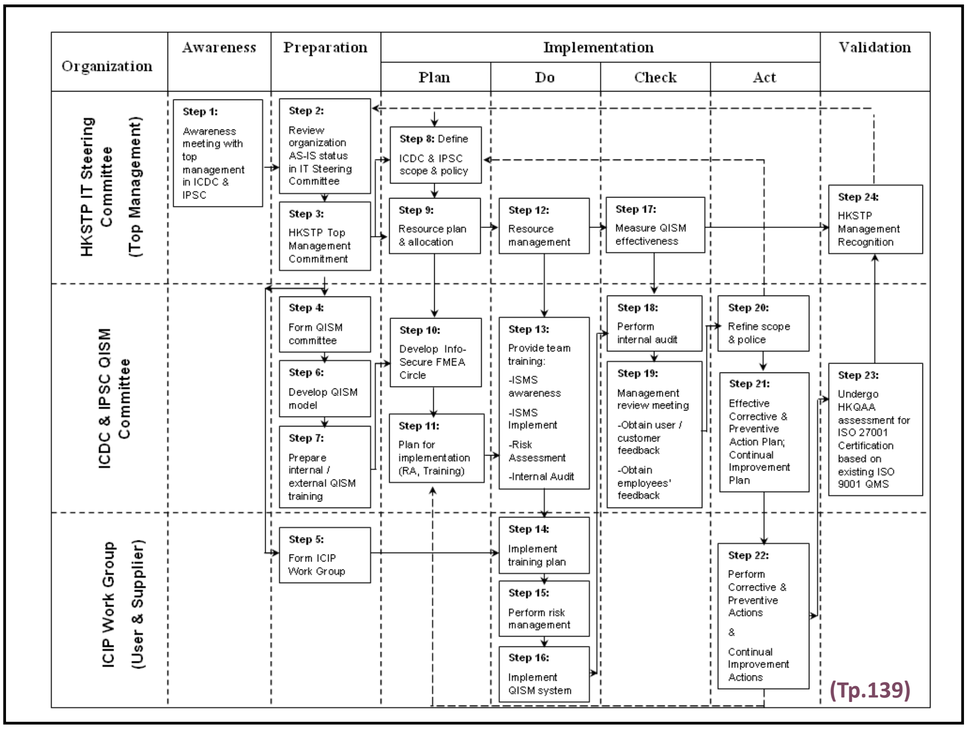
# The Chamber Concept



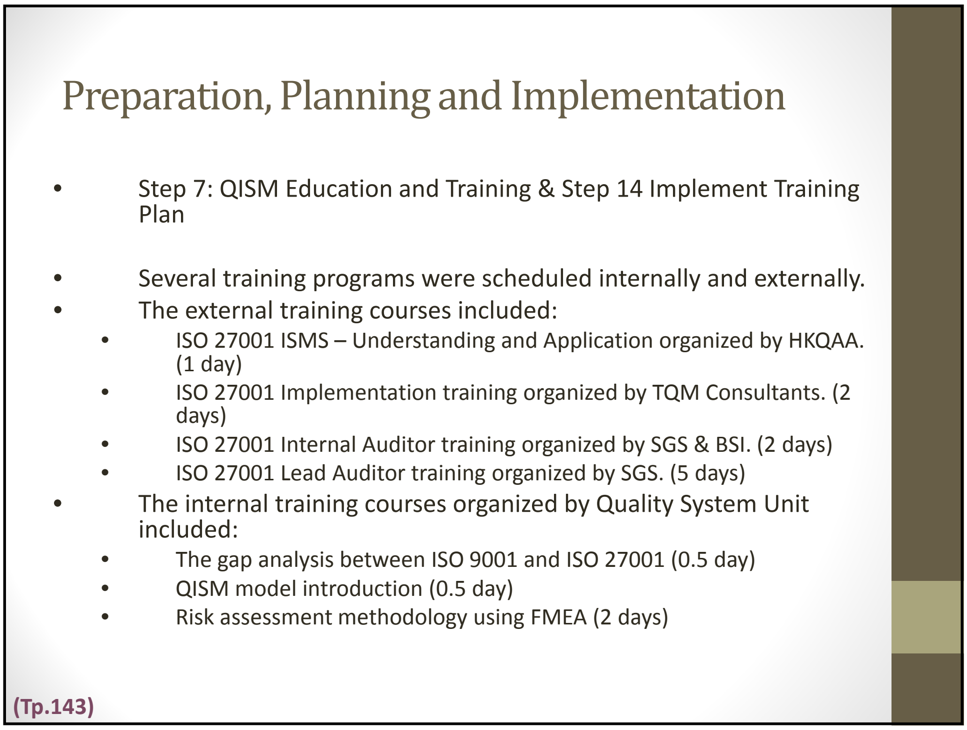
An ideal solution be…
in a clean environment…
you can work on it but…
you cannot take it away…

# ISO 27001 Certified Virtual IP Chamber




Organization
Awareness
Preparation
Implementation
Plan
Do
Check
Act
Validation
HKSTP IT Steering Committee (Top Management)
ICDC & IPSC QISM Committee
ICIP Work Group (User & Supplier)
Step 1: Awareness meeting with top management in ICDC & IPSC
Step 2: Review organization AS-IS status in IT Steering Committee
Step 3: HKSTP Top Management Commitment
Step 4: Form QISM committee
Step 5: Form ICIP Work Group
Step 6: Develop QISM model
Step 7: Prepare internal / external QISM training
Step 8: Define ICDC & IPSC scope & policy
Step 9: Resource plan & allocation
Step 10: Develop Info-Secure FMEA Circle
Step 11: Plan for implementation (RA, Training)
Step 12: Resource management
Step 13: Provide team training: -ISMS awareness -ISMS Implement -Risk Assessment -Internal Audit
Step 14: Implement training plan
Step 15: Perform risk management
Step 16: Implement QISM system
Step 17: Measure QISM effectiveness
Step 18: Perform internal audit
Step 19: Management review meeting -Obtain user / customer feedback -Obtain employees' feedback
Step 20: Refine scope & police
Step 21: Effective Corrective & Preventive Action Plan; Continual Improvement Plan
Step 22: Perform Corrective & Preventive Actions & Continual Improvement Actions
Step 23: Undergo HKQAA assessment for ISO 27001 Certification based on existing ISO 9001 QMS
Step 24: HKSTP Management Recognition

(Tp.139)



## Preparation, Planning and Implementation

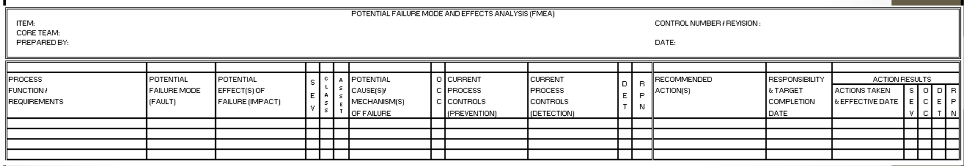
- Step 7: QISM Education and Training & Step 14 Implement Training Plan

- Several training programs were scheduled internally and externally.
- The external training courses included:
  - ISO 27001 ISMS – Understanding and Application organized by HKQAA. (1 day)
  - ISO 27001 Implementation training organized by TQM Consultants. (2 days)
  - ISO 27001 Internal Auditor training organized by SGS & BSI. (2 days)
  - ISO 27001 Lead Auditor training organized by SGS. (5 days)
- The internal training courses organized by Quality System Unit included:
  - The gap analysis between ISO 9001 and ISO 27001 (0.5 day)
  - QISM model introduction (0.5 day)
  - Risk assessment methodology using FMEA (2 days)

(Tp.143)

# Information Security FMEA (ICIP_WI_001) (I)

- Full name: Information Security Failure Mode and Effects Analysis (FMEA)
- Name of the process
- Name of the core team member
- Description/purpose of process 3



POTENTIAL FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

ITEM:
CORE TEAM:
PREPARED BY:

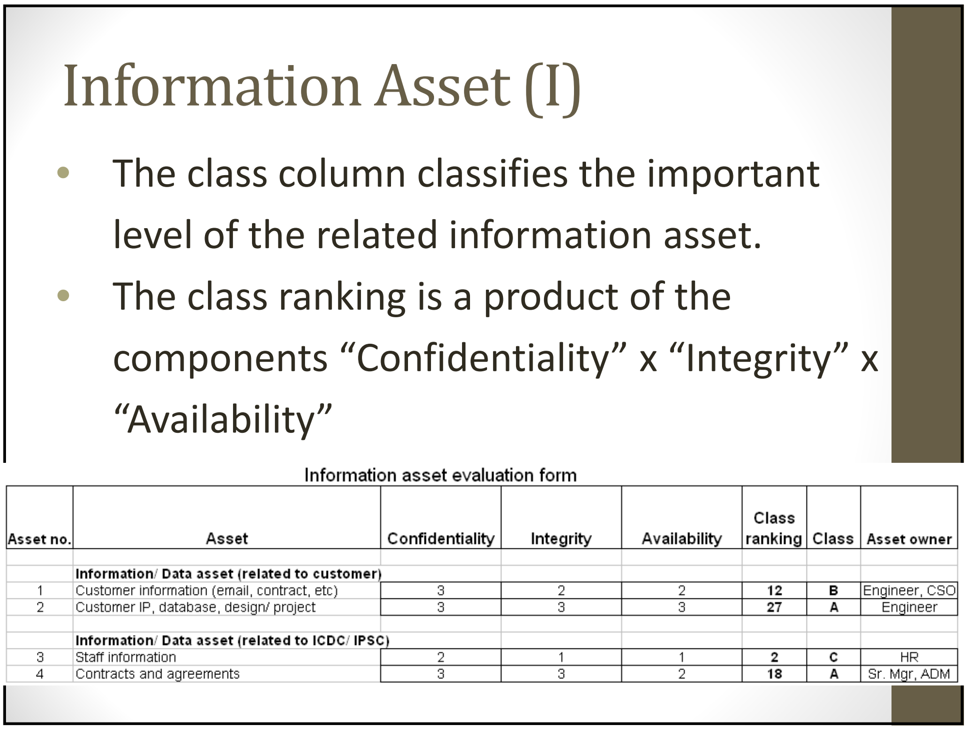
CONTROL NUMBER / REVISION :

DATE:

| PROCESS FUNCTION / REQUIREMENTS | POTENTIAL FAILURE MODE (FAULT) | POTENTIAL EFFECT(S) OF FAILURE (IMPACT) | SEV | CLASS | ASSET | 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 | ACTION RESULTS | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | ACTIONS TAKEN & EFFECTIVE DATE | SEV | OCC | DET | RPN |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |

# Information Security FMEA (ICIP_WI_001) (II)

- Enter the Potential Failure Mode
- Enter each Potential Effect of Failure in information security
- Enter Severity ranking of each effect to the customer (SEV)
- List potential cause of failure
- Enter Occurrence ranking (OCC)
- Enter Detection ranking of Current Process Controls (DET)

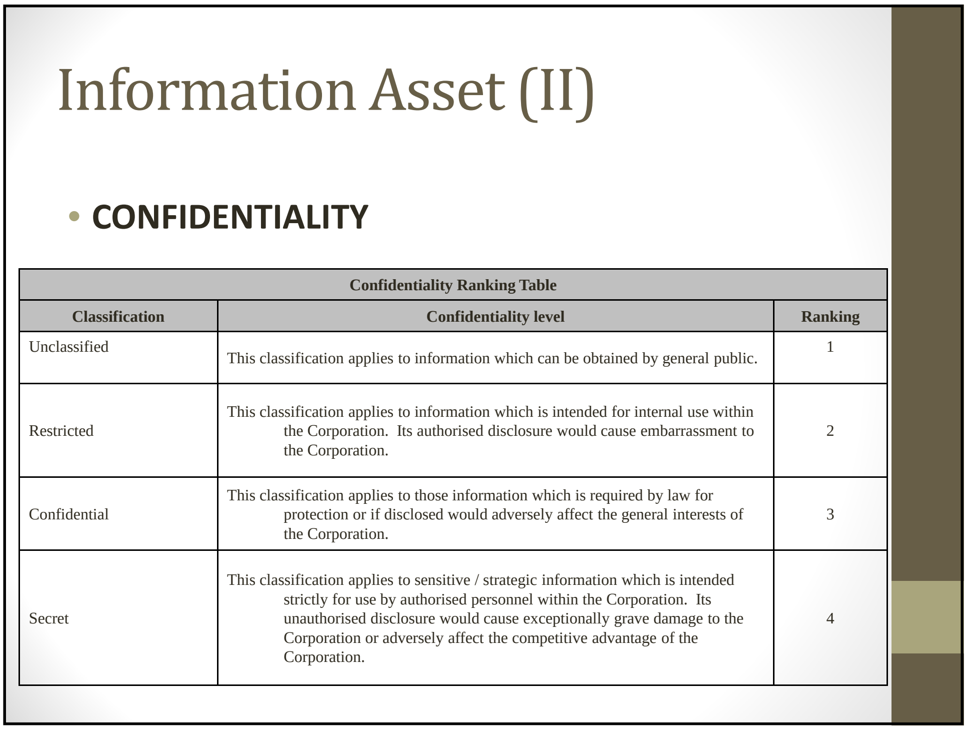


# Information Asset (I)

- The class column classifies the important level of the related information asset.
- The class ranking is a product of the components “Confidentiality” x “Integrity” x “Availability”

Information asset evaluation form

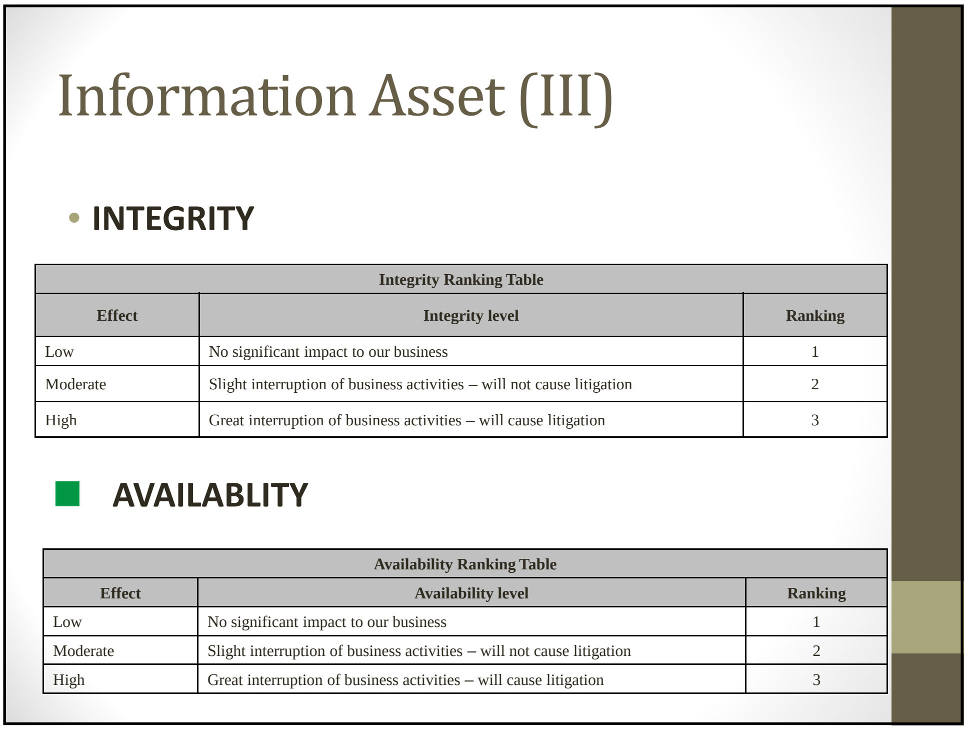
| Asset no. | Asset | Confidentiality | Integrity | Availability | Class ranking | Class | Asset owner |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | **Information/ Data asset (related to customer)** | | | | | | |
| 1 | Customer information (email, contract, etc) | 3 | 2 | 2 | **12** | **B** | Engineer, CSO |
| 2 | Customer IP, database, design/ project | 3 | 3 | 3 | **27** | **A** | Engineer |
| | | | | | | | |
| | **Information/ Data asset (related to ICDC/ IPSC)** | | | | | | |
| 3 | Staff information | 2 | 1 | 1 | **2** | **C** | HR |
| 4 | Contracts and agreements | 3 | 3 | 2 | **18** | **A** | Sr. Mgr, ADM |



# Information Asset (II)

- **CONFIDENTIALITY**

| Confidentiality Ranking Table | | |
|---|---|---|
| **Classification** | **Confidentiality level** | **Ranking** |
| Unclassified | This classification applies to information which can be obtained by general public. | 1 |
| Restricted | This classification applies to information which is intended for internal use within the Corporation. Its authorised disclosure would cause embarrassment to the Corporation. | 2 |
| Confidential | This classification applies to those information which is required by law for protection or if disclosed would adversely affect the general interests of the Corporation. | 3 |
| Secret | This classification applies to sensitive / strategic information which is intended strictly for use by authorised personnel within the Corporation. Its unauthorised disclosure would cause exceptionally grave damage to the Corporation or adversely affect the competitive advantage of the Corporation. | 4 |



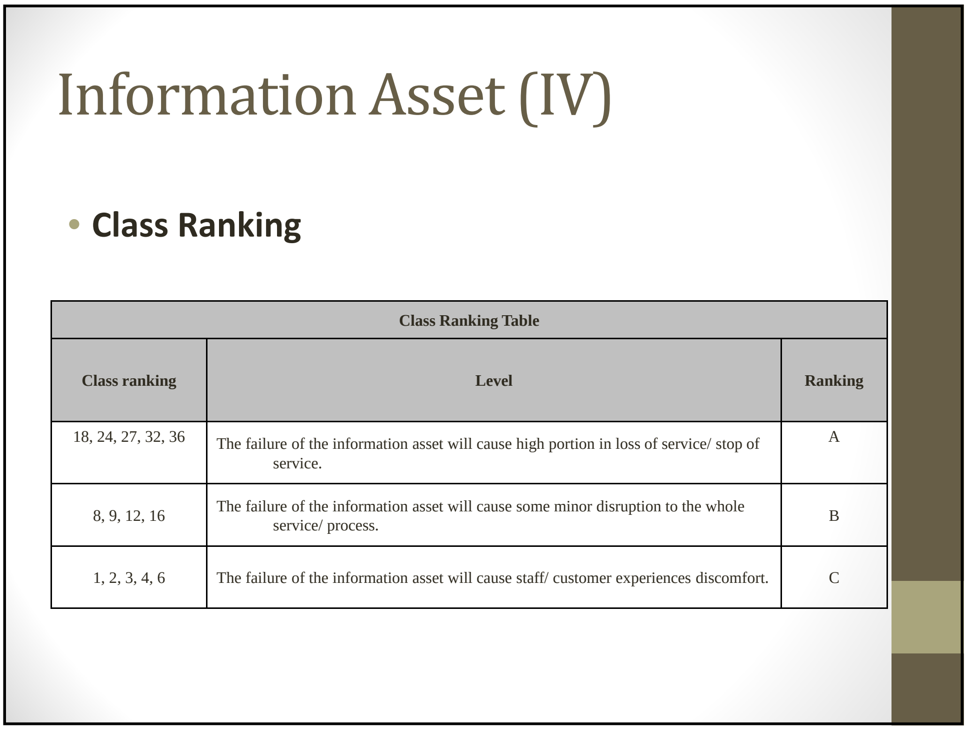
# Information Asset (III)

- **INTEGRITY**

| Integrity Ranking Table | | |
|---|---|---|
| **Effect** | **Integrity level** | **Ranking** |
| Low | No significant impact to our business | 1 |
| Moderate | Slight interruption of business activities – will not cause litigation | 2 |
| High | Great interruption of business activities – will cause litigation | 3 |

■ **AVAILABLITY**

| Availability Ranking Table | | |
|---|---|---|
| **Effect** | **Availability level** | **Ranking** |
| Low | No significant impact to our business | 1 |
| Moderate | Slight interruption of business activities – will not cause litigation | 2 |
| High | Great interruption of business activities – will cause litigation | 3 |



# Information Asset (IV)

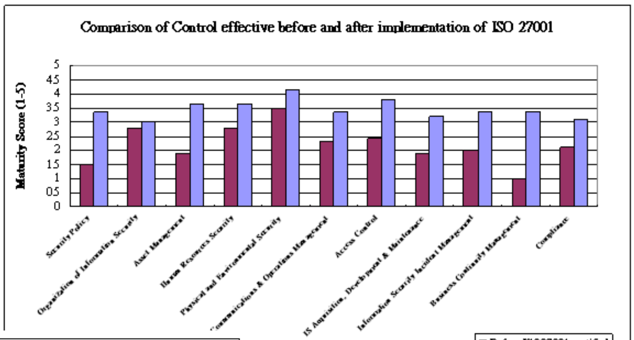
- **Class Ranking**

| Class Ranking Table | | |
|---|---|---|
| **Class ranking** | **Level** | **Ranking** |
| 18, 24, 27, 32, 36 | The failure of the information asset will cause high portion in loss of service/ stop of service. | A |
| 8, 9, 12, 16 | The failure of the information asset will cause some minor disruption to the whole service/ process. | B |
| 1, 2, 3, 4, 6 | The failure of the information asset will cause staff/ customer experiences discomfort. | C |

# Risk Priority Number (RPN)

- Enter Risk Priority Number (RPN) which is the product of Severity (S), Occurrence (O) and Detection (D) rankings.
- RPN = (S) x (O) x (D)
- Records:
  - Information Security FMEA Form, and
  - Information Asset Evaluation Form

# Internal Validation



ırity Audits Score Histogram after implementation of QISM model

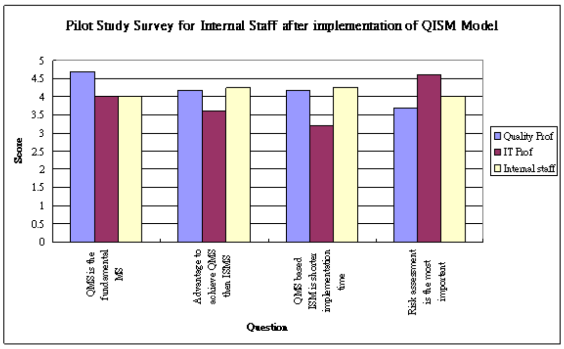
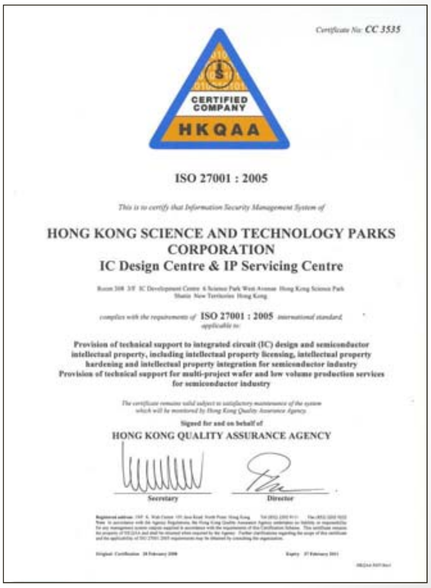


Figure 4.4.1-2 The result of Internal Staff on Pilot Study Survey

**(Tp.153)**

# External Validation

- The ISO 27001 certificate of ICDC and IPSC was granted in March 2008.



Certificate No: CC 3535

CERTIFIED COMPANY

HKQAA

ISO 27001 : 2005

*This is to certify that Information Security Management System of*

**HONG KONG SCIENCE AND TECHNOLOGY PARKS CORPORATION**
**IC Design Centre & IP Servicing Centre**

Room 308 3/F IC Development Centre 6 Science Park West Avenue Hong Kong Science Park
Shatin New Territories Hong Kong

*complies with the requirements of* **ISO 27001 : 2005** *international standard, applicable to:*

**Provision of technical support to integrated circuit (IC) design and semiconductor intellectual property, including intellectual property licensing, intellectual property hardening and intellectual property integration for semiconductor industry**
**Provision of technical support for multi-project wafer and low volume production services for semiconductor industry**

*The certificate remains valid subject to satisfactory maintenance of the system which will be monitored by Hong Kong Quality Assurance Agency.*

Signed for and on behalf of
HONG KONG QUALITY ASSURANCE AGENCY

Secretary

Director

Registered address: [illegible] North Point, Hong Kong [illegible]
Note: In accordance with the Agency Regulations, the Hong Kong Quality Assurance Agency undertakes no liability or responsibility [illegible]

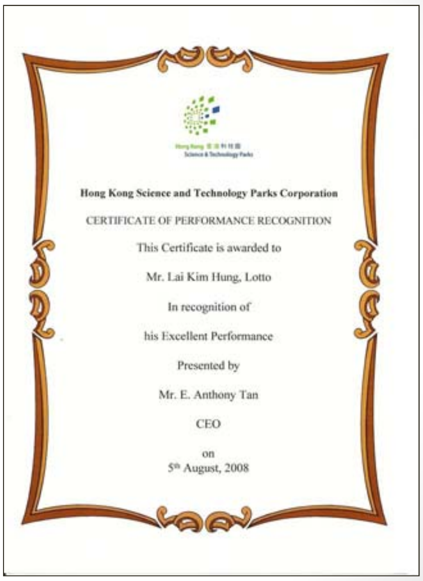
Original Certification: 28 February 2008

Expiry: 27 February 2011

(Tp.178)

# Top Management Recognition 2008

- Whole team members win the Excellent Performance Award based on this project.



Hong Kong 香港科技園
Science & Technology Parks

**Hong Kong Science and Technology Parks Corporation**

CERTIFICATE OF PERFORMANCE RECOGNITION

This Certificate is awarded to

Mr. Lai Kim Hung, Lotto

In recognition of

his Excellent Performance

Presented by

Mr. E. Anthony Tan

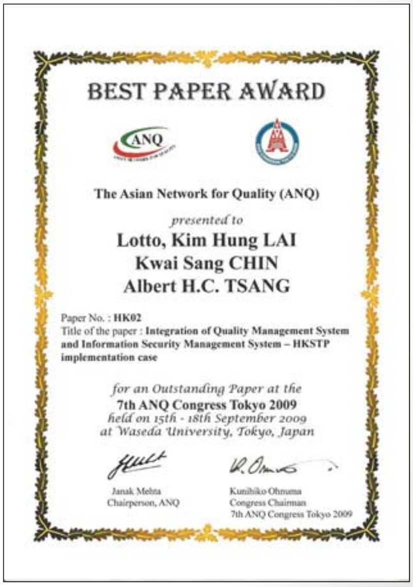
CEO

on

5th August, 2008

(Tp.180)

# Best Paper Award in ANQ 2009



BEST PAPER AWARD

The Asian Network for Quality (ANQ)

*presented to*

**Lotto, Kim Hung LAI**
**Kwai Sang CHIN**
**Albert H.C. TSANG**

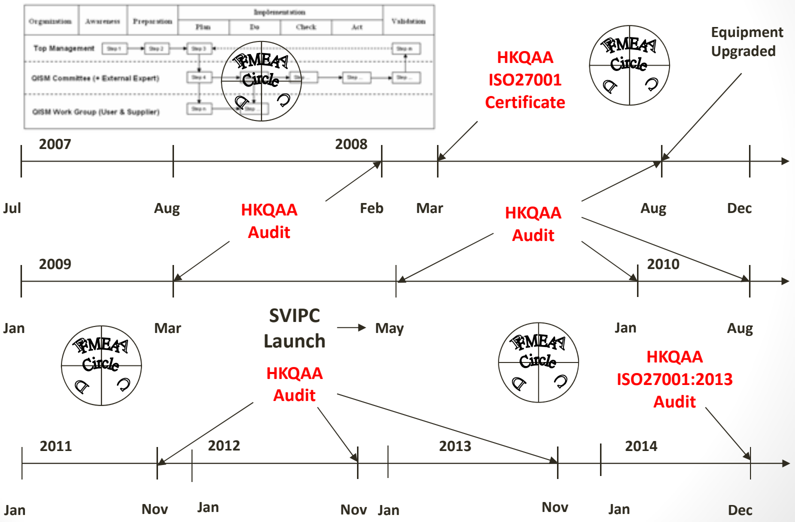
Paper No. : **HK02**
Title of the paper : **Integration of Quality Management System and Information Security Management System – HKSTP implementation case**

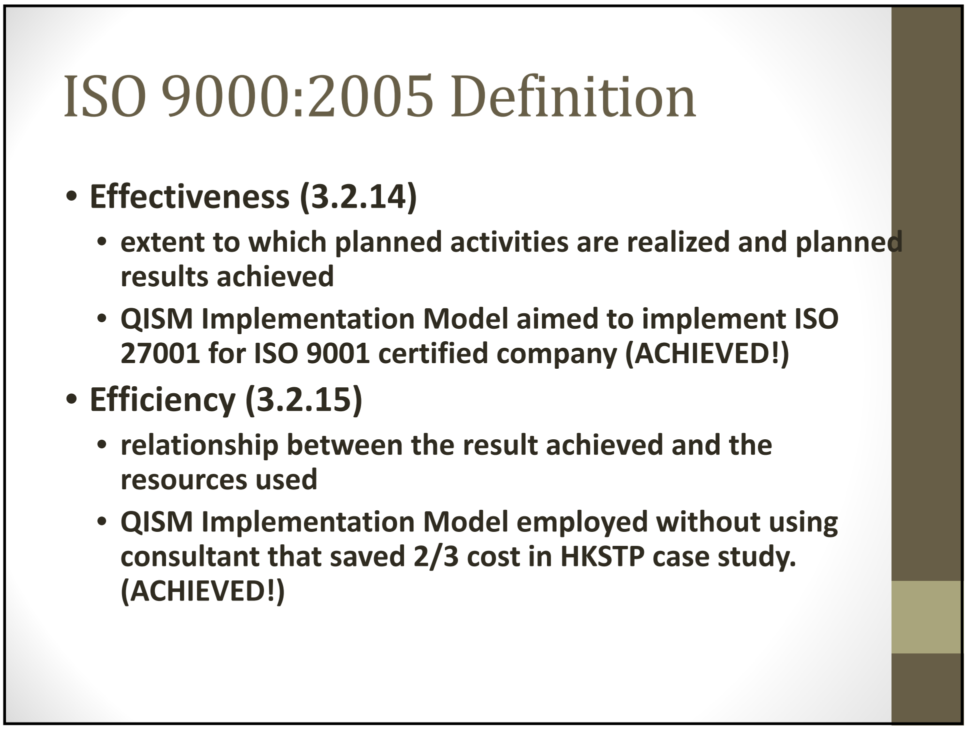
*for an Outstanding Paper at the*
**7th ANQ Congress Tokyo 2009**
*held on 15th - 18th September 2009*
*at Waseda University, Tokyo, Japan*

Janak Mehta
Chairperson, ANQ

Kunihiko Ohnuma
Congress Chairman
7th ANQ Congress Tokyo 2009

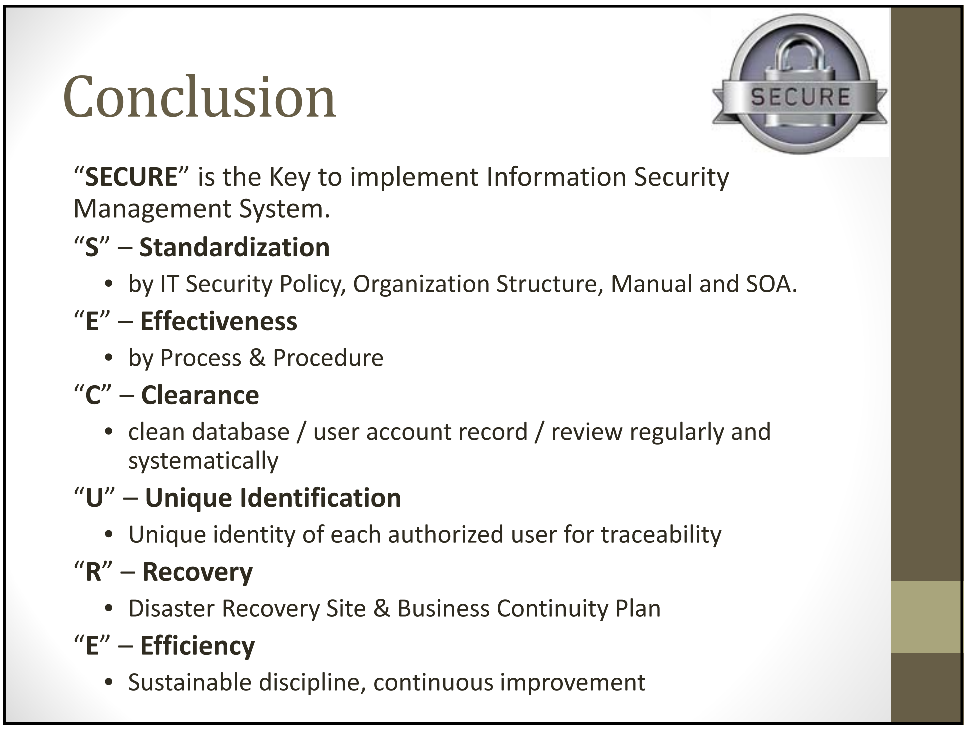
# QISM Implementation for 7 cycles





# ISO 9000:2005 Definition

- **Effectiveness (3.2.14)**
  - **extent to which planned activities are realized and planned results achieved**
  - **QISM Implementation Model aimed to implement ISO 27001 for ISO 9001 certified company (ACHIEVED!)**
- **Efficiency (3.2.15)**
  - **relationship between the result achieved and the resources used**
  - **QISM Implementation Model employed without using consultant that saved 2/3 cost in HKSTP case study. (ACHIEVED!)**



# Conclusion

“**SECURE**” is the Key to implement Information Security Management System.

“**S**” – **Standardization**

- by IT Security Policy, Organization Structure, Manual and SOA.

“**E**” – **Effectiveness**

- by Process & Procedure

“**C**” – **Clearance**

- clean database / user account record / review regularly and systematically

“**U**” – **Unique Identification**

- Unique identity of each authorized user for traceability

“**R**” – **Recovery**

- Disaster Recovery Site & Business Continuity Plan

“**E**” – **Efficiency**

- Sustainable discipline, continuous improvement