A large, detailed illustration of a maple leaf in shades of yellow and orange, positioned behind the title text.

個資保護風險管理與ISMS

Prepared by :
Mr. Simon Chen 陳昇智
TCIC Global Certification LTD.
Email: simon@mail.tcicgroup.com

Copyright © 2014 TCIC LTD ., All rights reserved.
All other trademarks are trademarks of their respective holders.
*Data sources are from indicated organizations in this presentation.



TCIC & Speaker



■ TCIC Global Certification Ltd. (TCIC) is a Canadian Registered Certification Body (RCB) accredited by APMG/itSMF under ISO20000 certification scheme and its ISO27001 Certification Services are accredited by BMWA (Vienna) and TAF (Taipei). Besides certification services, TCIC is an accredited training organization (ATO) under APMG/itSMF ISO20K scheme and a training provider for ISO2700X courses. TCIC in Taipei : 環奧國際驗證公司.

■ Speaker: Simon Chen 陳昇智

- ✓ ISO27001/ISO20000 Lead Auditor, TCIC-Canada
- ✓ APMG/itSMF Certified ISO20000 Auditor
- ✓ APMG/itSMF Certified ISO20000 Consultant
- ✓ ITIL Foundation Certificate
- ✓ Certified Information Security Manager, CIS-Austria
- ✓ ISO27001 Lead Auditor, CIS-Austria
- ✓ ISO20000 Lead Auditor, CIS-Austria
- ✓ Certified Information Systems Security Professional (CISSP)
- ✓ Project Management Professional (PMP)

- ✓ APMG/itSMF Accredited ISO20000 Course Lead Trainer
- ✓ Information Security Trainer, CIS-Austria
- ✓ Information Security Trainer, TCIC-Canada
- ✓ Car Connectivity Consortium (CCC) Auditor
- ✓ Auditor & Trainer 稽核師 & 講師



目錄



- 隱私權框架國際標準(ISO/IEC 29100:2011)簡介
- 風險管理相關國際標準簡介
- 新版ISMS國際標準(ISO/IEC 27001:2013)簡介及其對風險管理之要求
- 個資保護風險案例
- 個資保護風險管理

Data source of this presentation : ISO



A large, stylized maple leaf in shades of yellow and orange, positioned behind the title text.

隱私權框架國際標準 (ISO/IEC 29100:2011)簡介



ISO29100標準簡介



- Prepared by ISO/IEC JTC1/SC27
- Title - Information technology — Security techniques —
Privacy framework
- First edition published on the 2011-12-15
- Purpose of this International Standard – Provides a high-level framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems. It is general in nature and places organizational, technical, and procedural aspects in an overall privacy framework.



ISO/IEC 29100 – 目錄(Contents)



前言(Foreword)

簡介(Introduction)

1.範圍(Scope)

2.用語釋義(Terms and definitions)

3.符號和縮寫詞(Symbols and abbreviated terms)

4.隱私架構的基本元素(Basic elements of the privacy framework)

5.ISO 29100隱私原則(The privacy principles of ISO/IEC 29100)

Annex A (informative) Correspondence between ISO/IEC 29100 concepts and ISO/IEC 27000 concepts

ISO/IEC 29100 - Clause 2 用語釋義 (Terms and definitions)



- 2.1 anonymity
 - characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly
- 2.2 anonymization
 - process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

ISO/IEC 29100 - Clause 2 用語釋義 (Terms and definitions)



- 2.3 anonymized data
 - data that has been produced as the output of a personally identifiable information anonymization process
- ...
- 2.24 pseudonymization
 - process applied to personally identifiable information (PII) which replaces identifying information with an alias

ISO/IEC 29100 - Clause 2 用語釋義 (Terms and definitions)



- 2.8 opt-in
 - process or type of policy whereby the personally identifiable information (PII) principal is required to take an action to express explicit, prior consent for their PII to be processed for a particular purpose
- 2.9 personally identifiable information (PII)
 - any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

ISO/IEC 29100 - Clause 2 用語釋義 (Terms and definitions)



- 2.10 PII controller
 - privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes
- 2.11 PII principal
 - natural person to whom the personally identifiable information (PII) relates

ISO/IEC 29100 - Clause 2 用語釋義 (Terms and definitions)



- 2.12 PII processor
 - privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

- 2.15 privacy enhancing technology (PET)
 - privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system

ISO/IEC 29100 - Clause 3 符號和縮寫詞 (Symbols and abbreviated terms)



- ICT Information and Communication Technology
- PET Privacy Enhancing Technology
- PII Personally Identifiable Information



ISO/IEC 29100 - Clause 4 隱私架構的基本元素 (Basic elements of the privacy framework)



Table 1 – Possible flows of PII among the PII principal, PII controller, PII processor and a third party and their roles

	PII principal	PII controller	PII processor	Third party
Scenario a)	PII provider	PII recipient	—	—
Scenario b)	—	PII provider	PII recipient	—
Scenario c)	PII provider	—	PII recipient	—
Scenario d)	PII recipient	PII provider	—	—
Scenario e)	PII recipient	—	PII provider	—
Scenario f)	—	PII recipient	PII provider	—
Scenario g)	—	PII provider	—	PII recipient
Scenario h)	—	—	PII provider	PII recipient

ISO/IEC 29100 - Clause 4 隱私架構的基本元素(Basic elements of the privacy framework)



Table 2 – Example of attributes that can be used to identify natural persons

Examples
Age or special needs of vulnerable natural persons
Allegations of criminal conduct
Any information collected during health services
Bank account or credit card number
Biometric identifier
Credit card statements
Criminal convictions or committed offences
Criminal investigation reports
Customer number
Date of birth
Diagnostic health information
Disabilities
Doctor bills
Employees' salaries and human resources files
Financial profile
Gender
GPS position
GPS trajectories
Home address
IP address
Location derived from telecommunications systems
Medical history
Name
National identifiers (e.g., passport number)
Personal e-mail address
Personal identification numbers (PIN) or passwords
Personal interests derived from tracking use of internet web sites
Personal or behavioural profile
Personal telephone number
Photograph or video identifiable to a natural person
Product and service preferences
Racial or ethnic origin
Religious or philosophical beliefs
Sexual orientation
Trade-union membership
Utility bills

ISO/IEC 29100 - Clause 4 隱私架構的基本元素 (Basic elements of the privacy framework)

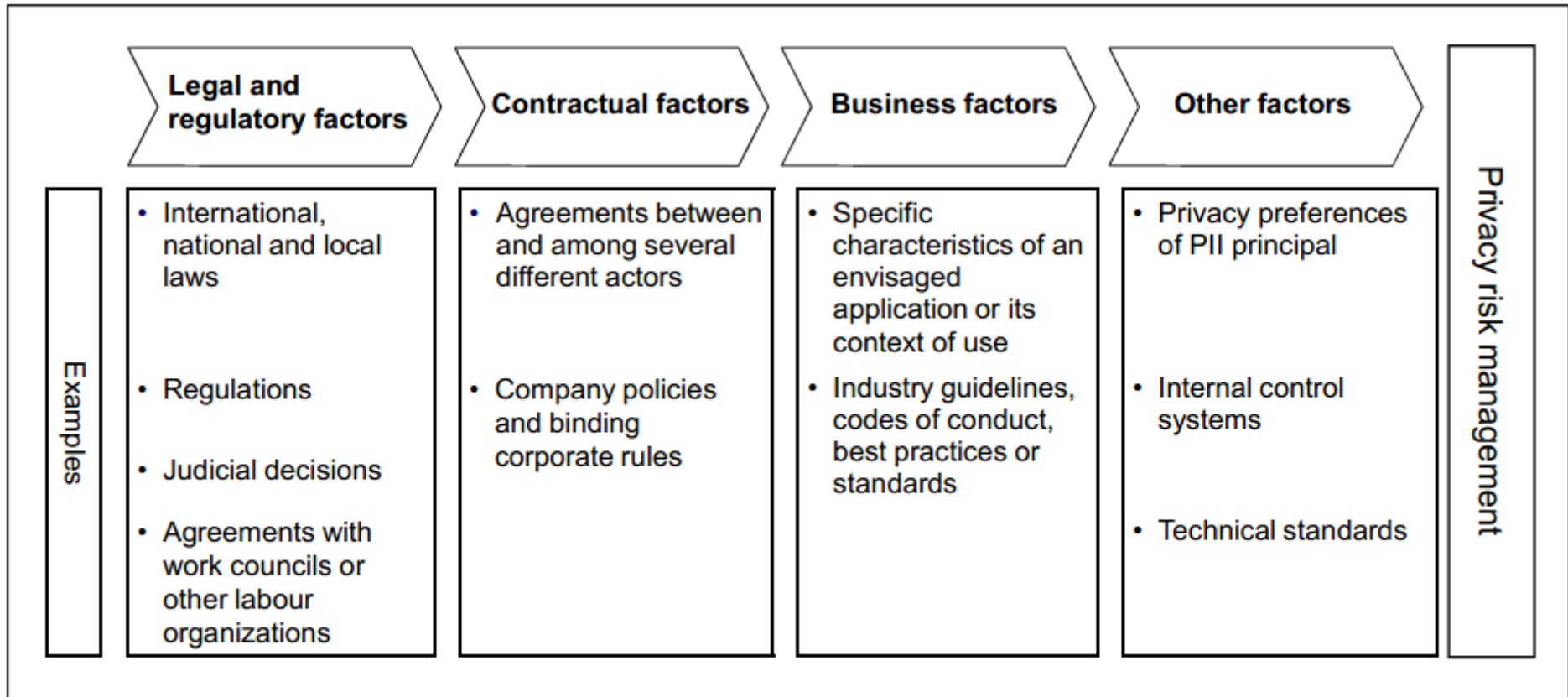


Figure 1 – Factors influencing privacy risk management

ISO/IEC 29100 - Clause 5 ISO 29100 隱私原則 (The privacy principles of ISO/IEC 29100)



Table 3 – The privacy principles of ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance



ISO/IEC 29100 - Annex A (informative)


Correspondence between ISO/IEC 29100 concepts and ISO/IEC 27000 concepts



Table A.1 — Matching ISO/IEC 29100 concepts to ISO/IEC 27000 concepts

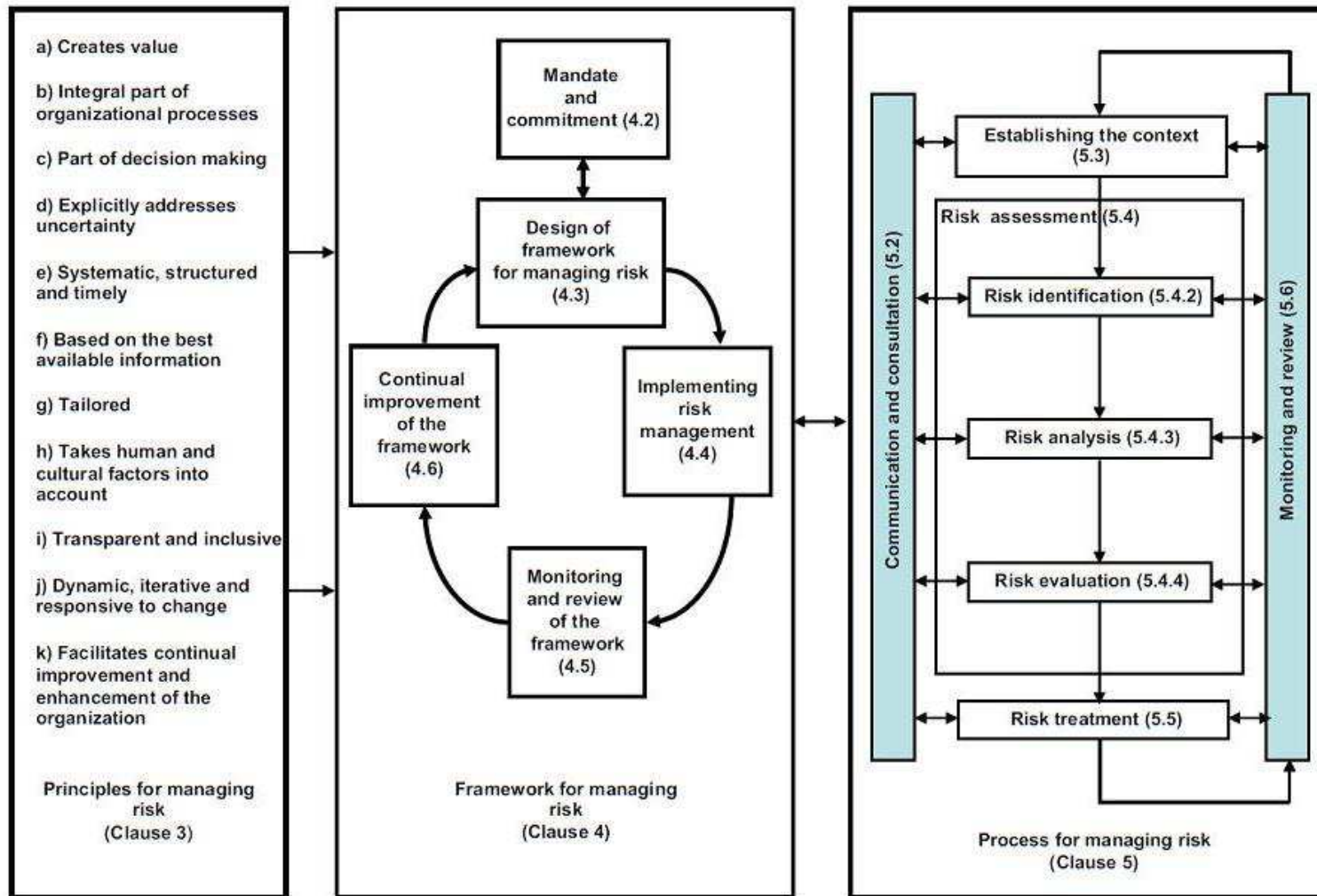
ISO/IEC 29100 concepts	Correspondence with ISO/IEC 27000 concepts
Privacy stakeholder	Stakeholder
PII	Information asset
Privacy breach	Information security incident
Privacy control	Control
Privacy risk	Risk
Privacy risk management	Risk management
Privacy safeguarding requirements	Control objectives

ISO29100 is the right international model to integrate Risk Management + PIA together with ISO27001.



風險管理相關標準簡介

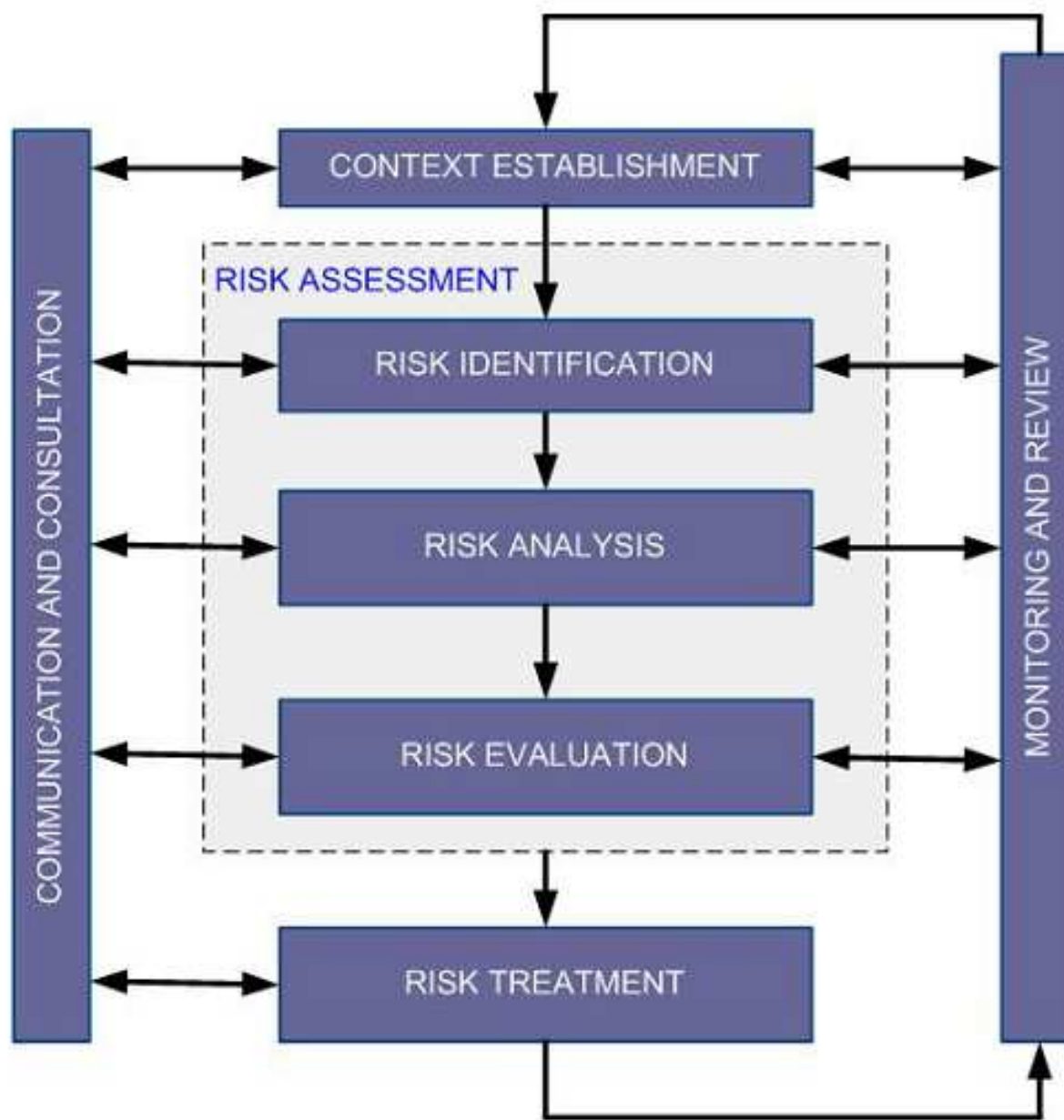
ISO 31000 Risk management -- Principles and guidelines



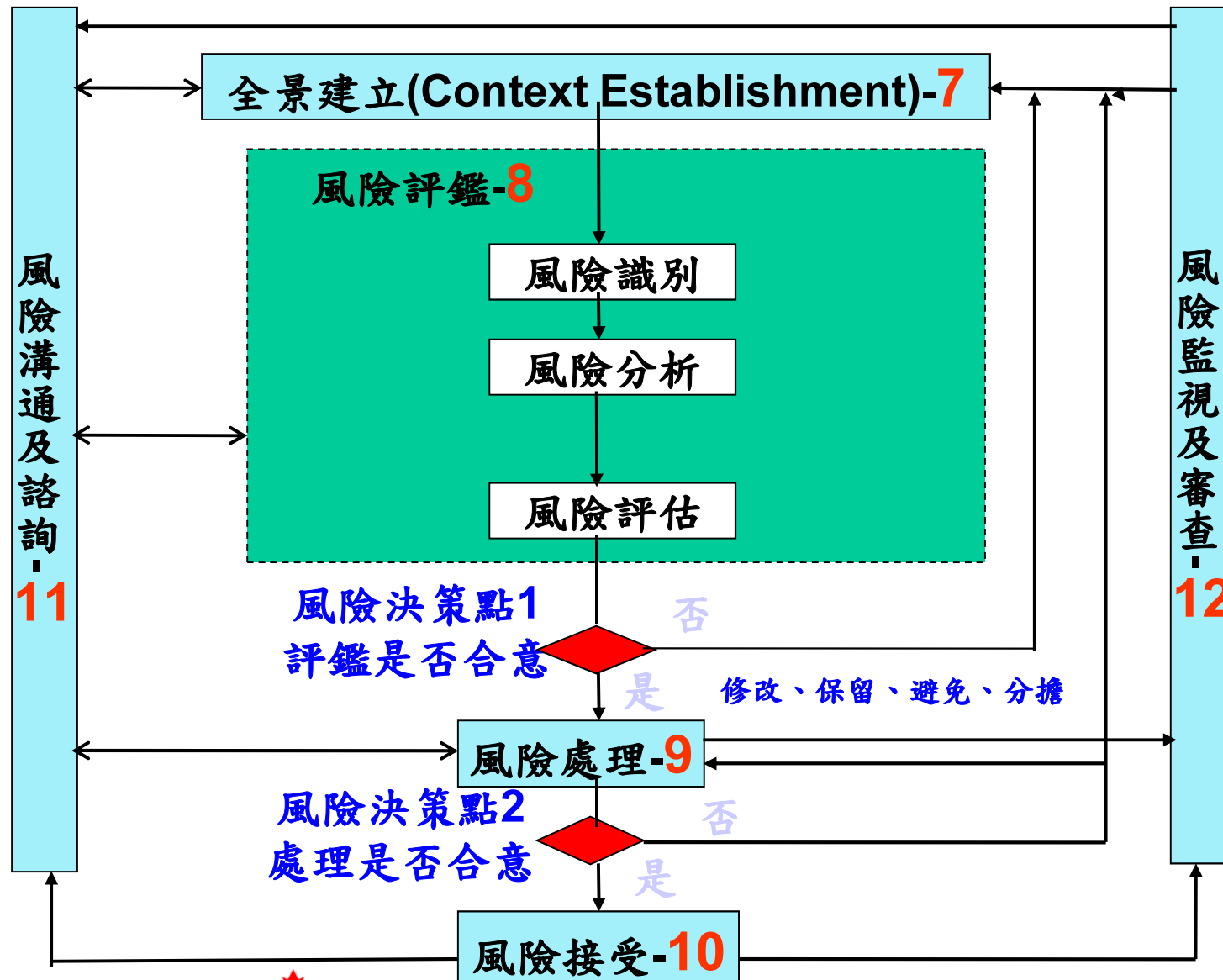
ISO31000 : Relationships between the risk management principles, framework and process



ISO/IEC
27005 -
Clause 6
資訊安全風
險管理過程
總論
(Overview
of the ISRM
Process)



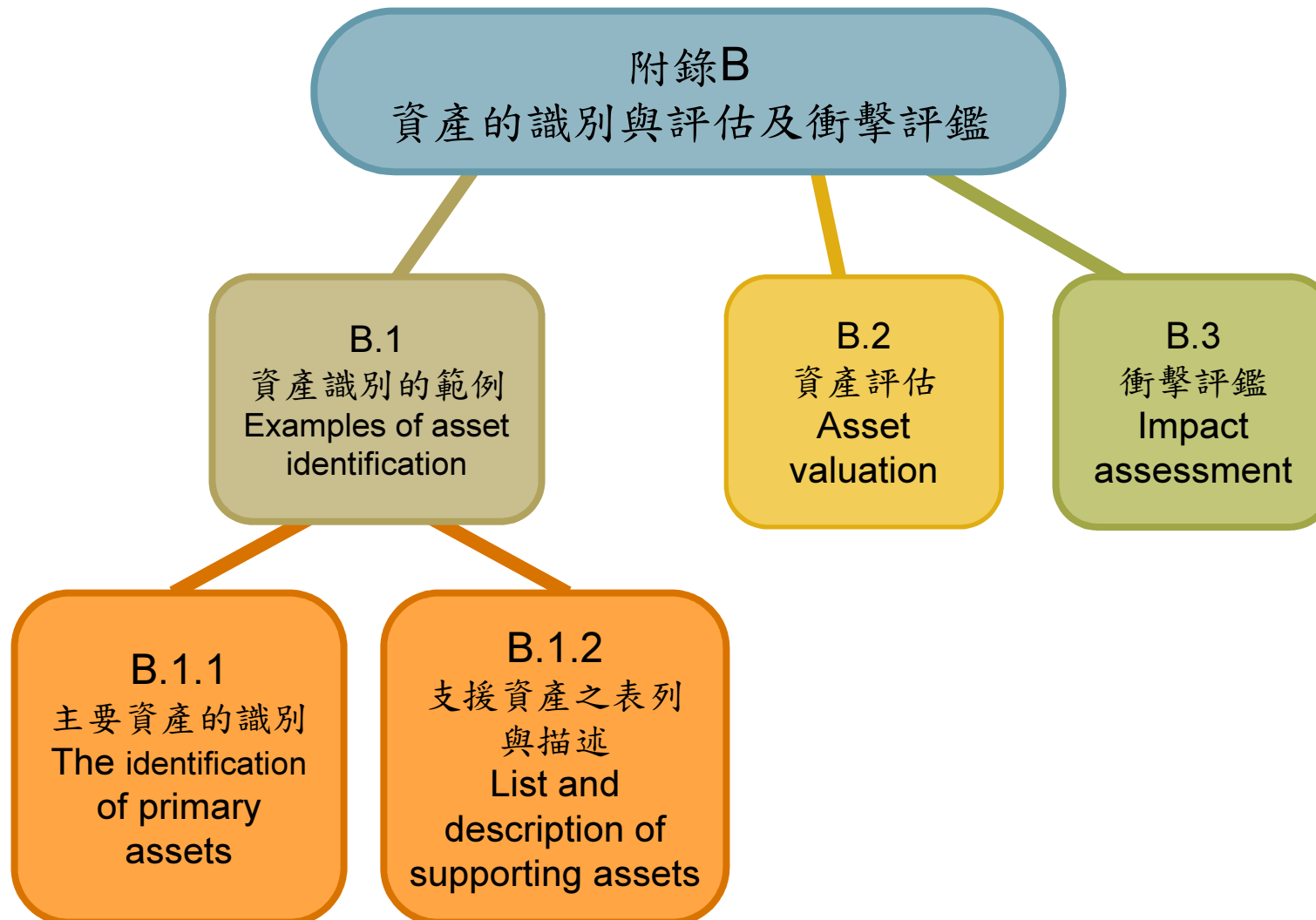
ISO/IEC 27005 風險管理過程



ISO/IEC 27005 - 附錄B(Annex B)

資產的識別與評估及衝擊評鑑

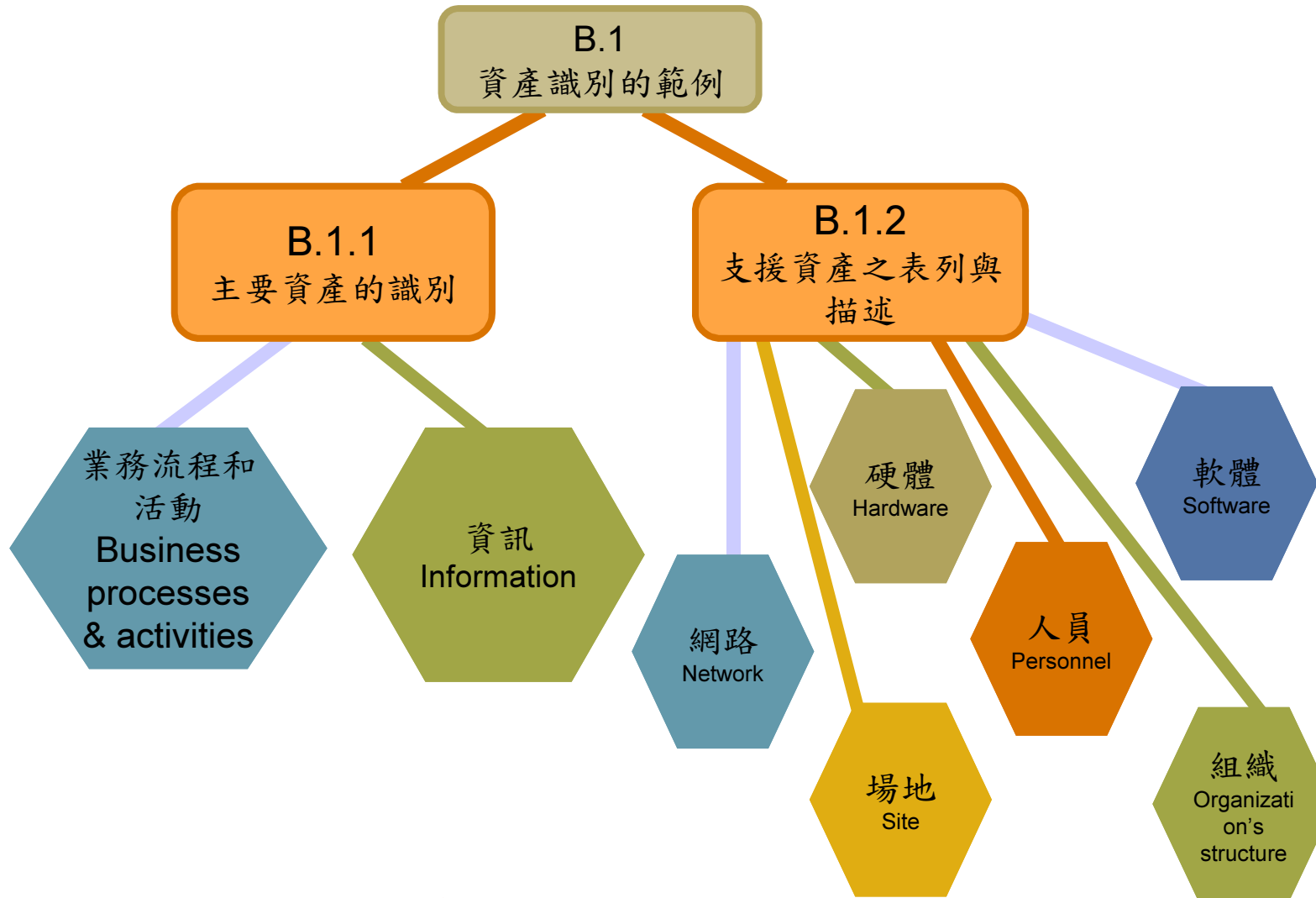
Identification and valuation of assets and impact assessment



ISO/IEC 27005 - 附錄B(Annex B)

資產的識別與評估及衝擊評鑑

Identification and valuation of assets and impact assessment



ISO/IEC 27005 - 附錄D(Annex D)

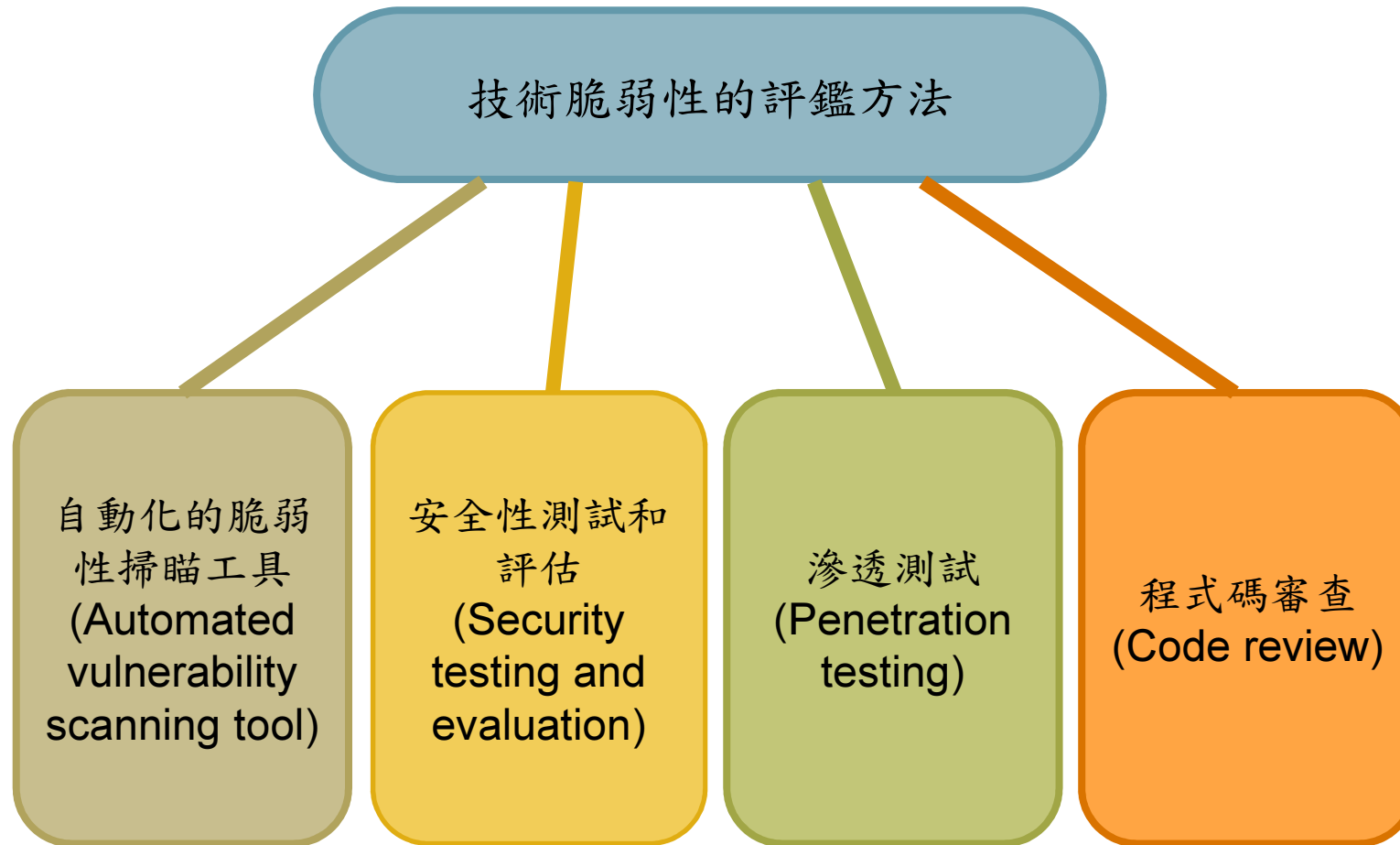



脆弱性和脆弱性評鑑的方法

Vulnerabilities and methods for vulnerability assessment

D.2 技術脆弱性的評鑑方法

Methods for assessment of technical vulnerabilities



A large, stylized maple leaf in shades of yellow and orange is positioned behind the title text.

新版ISMS國際標準 (ISO/IEC 27001:2013) 簡介及其對風險管理之要求



ISO/IEC 27001:2013標準簡介



- Prepared by ISO/IEC JTC1/SC27
- Title - Information technology — Security techniques — Information security management systems - Requirements
- First edition published on the 2005-06-15
- Second edition published on the 2013-10-01
- Purpose of this International Standard – to provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS).

ISO/IEC 27001:2013

標準簡介

ISO/IEC 27001:2013

Information technology -- Security techniques -- Information security management systems -- Requirements

General Information	Revisions	Corrigenda / Amendments
Edition: 2 (Monolingual)		ICS: 35.040
Status: <input checked="" type="checkbox"/> Published		Stage: 60.60 (2013-09-25)
TC/SC: ISO/IEC JTC 1/SC 27		Number of Pages: 23



ISO/IEC 27001:2013標準簡介



This International Standard applies the **high-level structure, identical sub-clause titles, identical text, common terms, and core definitions (Appendix 2)** defined in Annex SL of **ISO/IEC Directives, Part 1**, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

Annex SL (normative)

Proposals for management system standards

Appendix 1 (normative) Justification criteria questions

Appendix 2 (normative) High level structure, identical core text, common terms and core definitions

Appendix 3 (informative) Guidance on high level structure, identical core text, common terms and core definitions

ISO/IEC 27001:2013標準簡介



SL.5.1

See Appendix 2 Clause 3.04
management system

set of interrelated or interacting elements of an organization (3.01) to establish policies (3.07) and objectives (3.08) and processes (3.12) to achieve those objectives

SL.5.2

MSS - Management System Standard

Standard that provides requirements or guidelines for organizations to develop and systematically manage their policies, processes and procedures in order to achieve specific objectives.

NOTE 1

An effective management system is usually based on managing the organization's processes using a "Plan-Do-Check-Act" approach in order to achieve the intended outcomes

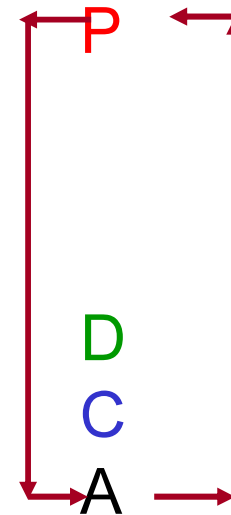


ISO/IEC 27001:2013標準簡介



Appendix 2 (normative) High level structure, identical core text, common terms and core definitions

- 0. Introduction
- 1. Scope
- 2. Normative references
- 3. Terms and definition
- 4. Context of the organization
- 5. Leadership
- 6. Planning
- 7. Support
- 8. Operation
- 9. Performance evaluation
- 10. Improvement



ISO/IEC 27001:2013標準簡介

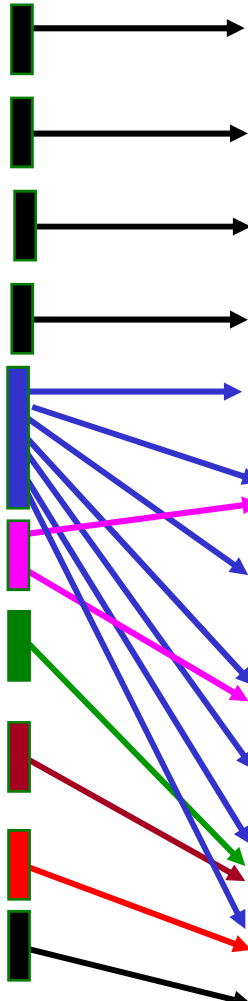


ISO/IEC 27001:2005

0. Introduction
1. Normative references
2. Scope
3. Terms and definition
4. Information security management system
5. Management responsibility
6. Internal ISMS audits
7. Management review of the ISMS
8. ISMS improvement
Annex A

ISO/IEC 27001:2013

0. Introduction
1. Normative references
2. Scope
3. Terms and definition
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement
Annex A



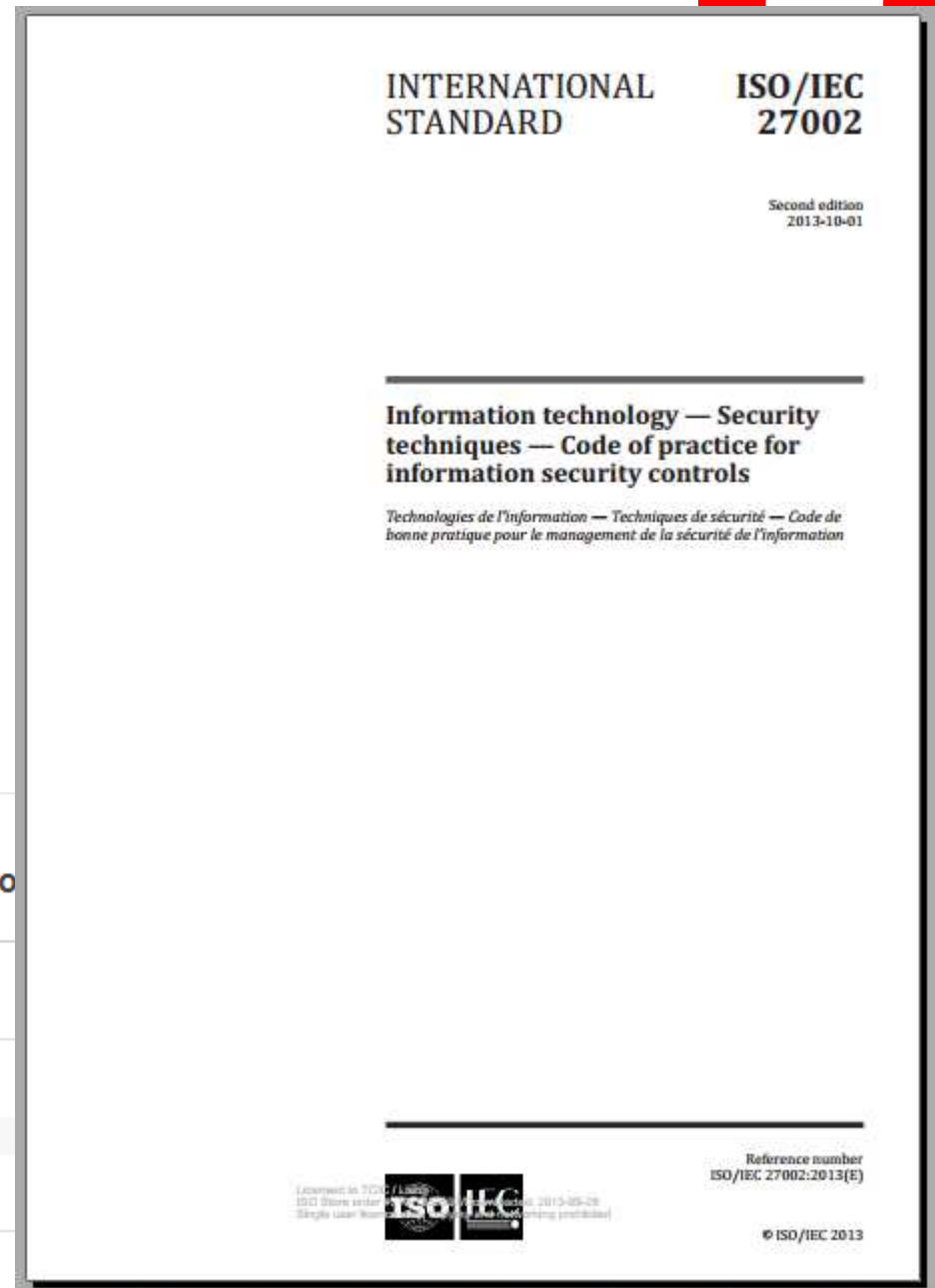
ISO/IEC 27002:2013標準簡介



- Prepared by ISO/IEC JTC1/SC27
- Title - Information technology — Security techniques —
Code of practice for information security controls
- First edition published on the 2005-06-15
- Second edition published on the 2013-10-01
- Purpose of this International Standard – Designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as a guidance document for organizations implementing commonly accepted information security controls.

ISO/IEC 27002:2013

標準簡介



ISO/IEC 27002:2013

Information technology -- Security techniques -- Code of practice for information security controls

General information	Revisions	Corrigenda / Amendments
Edition: 2 (Monolingual)		ICS: 35.040
Status: ✓ Published		Stage: 60.60 (2013-09-25)
TC/SC: ISO/IEC JTC 1/SC 27		Number of Pages: 80



ISO/IEC 27002:2013標準簡介



- ISO/IEC 27001:2005原區分為11個條款(clauses)、39個分類(categories)、133項控制措施(controls)，新版則調整為14個條款(clauses)、35個分類(categories)、114項控制措施(controls)；雖然條款(clauses)數量增加，但分類與控制措施則因整併後減少。
- 新版各個條款(clauses)所包括的分類(categories)與控制措施(controls)，以及與ISO/IEC 27001:2005的比照如后：



ISO/IEC 27002:2013 (14 clauses)

條款	名稱	分類	控制措施
5	Information security policies 資訊安全政策	1	2
6	Organization of information security 資訊安全之組織	2	7
7	Human resource security 人力資源安全	3	6
8	Asset management 資產管理	3	10
9	Access control 存取控制	4	14
 10	Cryptography 密碼學	1	2
11	Physical and environmental security 實體及環境安全	2	15
 12	Operations security 運作安全	7	14
 13	Communications security 通訊安全	2	7
14	System acquisition, development and maintenance 系統獲取、開發及維護	3	13
 15	Supplier relationships 供應者關係	2	5
16	Information security incident management 資訊安全事故管理	1	7
17	Information security aspects of business continuity management 營運持續管理之資訊安全層面	2	4
18	Compliance 遵循性	2	8
		35	114

ISO/IEC 27002:2013與2005版章節比較



ISO/IEC 27002:2005 (11 clauses)		ISO/IEC 27002:2013(14 clauses)	
條款	名稱	條款	名稱
5	Security Policy 安全政策	5	Information security policies 資訊安全政策
6	Organization of Information Security 資訊安全組織	6	Organization of information security 資訊安全之組織
7	Asset Management 資產管理	7	Human resource security 人力資源安全
8	Human Resources Security 人力資源安全	8	Asset management 資產管理
9	Physical & Environmental Security 實體及環境安全	9	Access control 存取控制
10	Communications & Operations Management 通訊與作業管理	10	Cryptography 密碼學
11	Access Control 存取控制	11	Physical and environmental security 實體及環境安全
		12	Operations security 運作安全
		13	Communications security 通訊安全

ISO/IEC 27002:2013與2005版章節比較



ISO/IEC 27002:2005 (11 clauses)		ISO/IEC 27002:2013(14 clauses)	
條款	名稱	條款	名稱
12	Information Systems Acquisition, Development and Maintenance 資訊系統獲取、開發及維護		
13	Information Security Incident Management 資訊安全事故管理		
14	Business Continuity Management 營運持續管理	14	System acquisition, development and maintenance 系統獲取、開發及維護
15	Compliance 遵循性	15	Supplier relationships 供應者關係
		16	Information security incident management 資訊安全事故管理
		17	Information security aspects of business continuity management 營運持續管理之資訊安全層面
		18	Compliance 遵循性

ISO/IEC 27002:2013



條款	名稱	新的控制措施
5	Information security policies 資訊安全政策	
6	Organization of information security 資訊安全之組織	1
7	Human resource security 人力資源安全	
8	Asset management 資產管理	
9	Access control 存取控制	2
10	Cryptography 密碼學	
11	Physical and environmental security 實體及環境安全	
12	Operations security 運作安全	1
13	Communications security 通訊安全	
14	System acquisition, development and maintenance 系統獲取、開發及維護	4
15	Supplier relationships 供應者關係	1
16	Information security incident management 資訊安全事故管理	2
17	Information security aspects of business continuity management 營運持續管理之資訊安全層面	1
18	Compliance 遵循性	
		12

A large, semi-transparent maple leaf with yellow and orange autumn colors is centered behind the text.

ISO/IEC 27001:2013標準 對風險管理要求



6 Planning 規畫



6.1 Actions to address risks and opportunities

解決風險和機遇的行動

6.1.1 General

✓When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed

- a) ensure the information security management system can achieve its intended outcome(s);
- b) prevent, or reduce, undesired effects; and
- c) achieve continual improvement.



6 Planning 規畫



- ✓ The organization shall plan:
 - d) actions to address these risks and opportunities; and
 - e) how to
 - 1) integrate and implement the actions into its information security management system processes; and
 - 2) evaluate the effectiveness of these actions.



6 Planning 規劃



6.1.2 Information security risk assessment

- ✓ The organization shall define **and apply** an information security risk assessment process that:
 - a) establishes and maintains information security risk criteria **that include:**
 - 1) the risk acceptance criteria; and
 - 2) criteria for performing information security risk assessments;
 - b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

6 Planning 規畫



- c) identifies the information security risks:
 - 1) apply the information security risk assessment process to **identify risks** associated with the **loss of confidentiality, integrity and availability for information** within the scope of the information security management system; and
 - 2) identify the **risk owners**;

- d) analyses the information security risks:
 - 1) assess the potential consequences that would result if the risks identified in 6.1.2c) 1) were to materialize;
 - 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2c) 1); and
 - 3) determine the levels of risk;

6 Planning 規劃



- e) evaluates the information security risks:
 - 1) compare the results of risk analysis with the risk criteria established in 6.1.2a); and
 - 2) prioritize the analysed risks for risk treatment.

- ✓ The organization shall retain documented information about the information security risk assessment process.

6 Planning 規畫



6.1.3 Information security risk treatment

✓The organization shall define and apply an information security risk treatment process to:

- a) select appropriate information security risk treatment options, taking account of the risk assessment results;
- b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE Organizations can design controls as required, or identify them from any source.



6 Planning 規劃



- c) compare the controls determined in 6.1.3b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 1: Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no **necessary controls** are overlooked

NOTE 2: Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls **may be needed**.

6 Planning 規畫



- d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 a), b) and c)) and justification for inclusions, **whether they are implemented or not**, and the justification for exclusions of controls **from** Annex A;
- e) formulate an information security risk treatment plan; **and**
- f) obtain **risk owners'** approval of the information security risk treatment plan and acceptance of the residual information security risks.

- ✓ The organization shall retain documented information about the information security risk treatment process.

NOTE The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in **ISO 31000**.

8 Operation 作業



8.1 Operational planning and control 作業規劃與控制

- ✓The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.
- ✓The organization shall also implement plans to achieve information security objectives determined in 6.2.
- ✓The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.
- ✓The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.
- ✓The organization shall ensure that outsourced processes are determined and controlled.



8 Operation 作業




8.2 Information security risk assessment 資訊安全風險評鑑

- ✓ The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).
- ✓ The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment 資訊安全風險處理

- ✓ The organization shall implement the information security risk treatment plan.
- ✓ The organization shall retain documented information of the results of the information security risk treatment.





個資保護風險案例

案例-1

廢棄文件管控失誤

醫院錯將病歷當便條紙

-08/08/2011



為了避免資源浪費及擷節成本，許多企業都設有廢紙回收箱，回收只有單面列印的A4紙張，做為列印紙或便條紙來用，這種做法雖然符合環保精神，但若管控不當，很可能造成資料外洩。日前，**某**醫院被民眾檢舉，服務台提供的便條紙背面竟然是另一名病患的就診資料，包括姓名、性別、年齡、體重、生日、看診日、及相關診斷與檢查結果，雖然**某**醫院事後清查，只有一張病歷資料外流，但對醫院形象已經造成嚴重影響。

先就事發原因來看，根據**某**醫院行政副院長**某**的說法，這張洩露病患隱私的便條紙，很可能是批價單。按照醫院看診流程，電腦列印出批價單之後，正本交給就診民眾、副本則貼在紙本病歷上保存，不過有時因為電腦問題，可能會多印或重印，這些多出來的表單就會被當成廢棄文件。

至於廢棄文件的處理也有一定程序。**某**醫院將廢棄文件分為機密與一般兩種類別，總務處負責收取各單位廢棄的機密文件，再委託業者銷毀，至於一般文件則做為影印回收紙或便條紙來使用。這次的意外應該是經手人員分錯類別，沒有經院內正常程序銷毀，

案例1-分析

- 主要資產：
 - 業務流程和活動：廢棄文件回收與銷毀流程
 - 資訊：含個資的紙張
- 支援資產：
 - 組織
 - 人員
 - 場地
- 風險擁有者(risk owners)：總務處



案例1-分析

- 風險：機密性－個資外洩
- 對應之ISO 27001:2013控制措施
 - A.6.1.1 information security roles and responsibilities 資訊安全角色與責任
 - A.7.2.2 Information security awareness, education and training 資訊安全認知、教育及訓練

案例1-分析



- A.8.2.2 Labelling of information 資訊的標示
- A.8.2.3 Handling of assets 資產的處置
- A.11.1.3 Securing offices, rooms and facilities 保全辦公室、房間及設施



案例-2



| 首頁 | 焦點新聞 | 資安知識庫 | 資安急診室 | 電子雜誌下載 | 資安二手市集 | 研討會 | 產業脈動

首頁 > 熱門新聞



NASA又傳員工筆電遭竊 至少萬筆個資外洩

作者：編輯部整理 -11/26/2012



日前美國NASA(美國國家航空暨太空總署)因為一名員工未加密的筆電遭竊，導致至少一萬筆個資外洩，為了避免類似情況再度發生，NASA下令內部所有筆電都必須加密，否則不准帶出NASA。

該起事件發生於10/31，NASA某位員工將筆電放在車內，雖然車子上了鎖，但依舊被偷走，該筆電硬碟中包含NASA員工、承包商等個人資料，雖然電腦使用了開機密碼鎖的保護機制，但是硬碟並沒有加密，電腦中某些特定檔案也未遵循NASA規範進行加密，另外，還有一些放在車上的NASA內部文件也同時被偷走。

NASA副署長Richard Keegan Jr.透過電子郵件向員工說明該起事件，並呼籲所有員工引以為誡，根據NASA現階段評估，至少有1萬人受到影響，但實際受影響人數應該更高。NASA說明，由於外洩的資料必須同時進行電子和人工的驗證分析，預估要60天左右才能確認所有受影響的人數。



案例2-分析

- 主要資產：
 - 業務流程和活動：Notebook攜出流程
 - 資訊：含個資的檔案
- 支援資產：
 - 組織
 - 人員
 - 硬體
 - 軟體
 - 場地



案例2-分析



- 風險擁有者(risk owners)：副署長
- 風險：機密性—個資外洩
- 對應之ISO 27001:2013控制措施
 - A.6.1.1 information security roles and responsibilities 資訊安全角色與責任
 - A.6.2.1 Mobile device policy 行動裝置政策
 - A.7.2.2 Information security awareness, education and training 資訊安全認知、教育及訓練

案例2-分析



- A.10.1.1 Policy on the use of cryptographic controls 使用密碼控制措施的政策
- A.11.2.5 Removal of assets 資產的攜出
- A.11.2.6 Security of equipment and assets off- premises 場所外設備與資產的安全



案例-3

藝陣被抹黑 屏縣府洩個資又搞烏龍

〔記者葉永騫／屏東報導〕屏東縣政府教育處最近發文給縣內各學校，要求加強關照參加民俗藝陣的學生，並附上一份民俗藝陣團體名冊，卻將負責人的前科也列上去，有的學校還將名冊上網公告，沒想到名冊資料擺烏龍，將負責人員冠上擄人勒贖前科，造成極大困擾。當事人為此向警局申請良民證自清，並痛罵縣府亂搞，揚言提告。

縣警局強調，曾因擄人勒贖案被移送，但檢察官裁定不起訴，資料上沒有任何犯罪紀錄，應該是教育處看不懂資料。

官員：輔導參考 沒要公告藝陣

縣府教育處學務科長則表示，該資料由縣警局提供，教育處發文給學校的用意，是提供給學校作為輔導與關切的參考，沒有要求學校公告，學校公告必須自負責任。

有鑒於學生參加八家將等民俗藝陣容易在校外引發暴力事件，教育處日前發文給縣內各級學校，要求校方對參加藝陣的學生多關懷與輔導，必要時可以請警察局少年隊協助，公文還附上一份民俗藝陣團體的名冊，把負責人電話和前科都註記在上面。

校方搞不清狀況 竟上網公告

有些學校接到教育處公文後，就直接將名冊公告到學校網站供家長參考，讓部分過去曾經犯錯的藝陣團體負責人感覺很受傷，更糟的是，有些人身家清白，也被縣府搞烏龍註記有前科。



案例3-分析

- 主要資產：
 - 業務流程和活動：跨組織資訊交換流程
 - 資訊：含個資的檔案
- 支援資產：
 - 組織
 - 人員
 - 軟體
 - 網路

案例3-分析



- 風險擁有者(risk owners)：教育處科長
- 風險：機密性—個資外洩
- 對應之ISO 27001:2013控制措施
 - A.7.2.2 Information security awareness, education and training 資訊安全認知、教育及訓練
 - A.10.1.1 Policy on the use of cryptographic controls 使用密碼控制措施的政策



案例3-分析



- A.13.2.2 Agreements on Information transfer
資訊傳遞協議
- A.13.2.3 Electronic messaging 電子傳訊



案例-4

金繳費中心網頁外洩個資，金管會限一周完成災情調查

文/iThome (記者) 2013-05-20

f 讚 92

f Share

g +1 2

+ 我要收藏

金網銀的繳費中心網頁出錯導致大量用戶個資外洩，甚至被Google搜尋引擎索引了而公開，坦言網頁出錯，回報金管會有33,000名用戶受影響，但否認個資外洩，金管會限1周內完成災情調查結果



客戶在ptt上揭露該銀行繳費中心發生外洩個資事件，從網路上流傳的網站畫面截圖可以看出，許多客戶包括姓名、手機、室內電話，甚至是信用卡號等資料，全部都遭到Google搜尋引擎的索引，都有個資外洩之虞。

新版個資法正式施行後，近日發生了第一起銀行個資外洩事件。



案例4-分析

- 主要資產：
 - 業務流程和活動：網站開發流程
 - 資訊：含個資的資料庫
- 支援資產：
 - 人員
 - 軟體
 - 網路



案例4-分析

- 風險擁有者(risk owners)：資訊中心主任
- 風險：機密性一個資外洩
- 對應之ISO 27001:2013控制措施
 - A.6.1.5 Information security in project management 專案管理的資訊安全



案例4-分析



- A.7.2.2 Information security awareness, education and training 資訊安全認知、教育及訓練
- A.14.2.8 System security testing 系統安全測試



案例-5

駭客用 webcam 偷窺,還謔稱被偷窺者是奴隸!!(下載分享軟體請當心被看光)

發表於 2013 年 06 月 21 日 由 Trend Labs 趨勢科技全球技術支援與研發中心

這兩天新聞報導淡江外籍男涉偷拍29人,被喻為土耳其版李宗瑞,女孩們不只在外交友要小心,即使坐在家裡都有可能被偷拍,看看以下案例:

[駭客打開女網友的webcam偷窺 「我喜歡糟蹋這些奴隸」](#) (英文版報導“[i enjoy messing with my girl slaves](#)”)看到這樣的報導,女孩們怎能不生氣呢?!

今天又看到一則[駭客入侵筆電 遙控偷拍辣妹洗澡](#)新聞,話說一名20歲的英國女大學生在浴室邊泡澡顛用筆電看電影,突然發現電腦鏡頭自動開啟,女大驚嚇了一跳,她懷疑電腦被駭客入侵,擔心自己在房內更衣和洗澡過程全都已經被人拍下。《英國廣播公司》(BBC)的調查指出,駭客利用各式吸引人的電郵,騙人點開有毒連結,之後利用中毒電腦的打開鏡頭後,偷拍電腦前的女性,然後將照片上傳到網路,甚至出售牟利。

幾年前也有一篇報導:[攝影機遭遠端遙控女子裸照PO上網](#),大意是說一名男大學生入侵某女子的電腦,再透過木馬程式網路遠端遙控,開啟女子電腦上的攝影機,並將該女子全裸出浴過程記錄,還入侵受害人部落格,將全裸影像上傳。其實這不是新病毒,早在2005年趨勢科技就曾發佈相關的[狗仔病毒\(WORM_RBOT.ASH\)](#),當時並沒有造成大流行。

但近年來這類病毒也開使用網頁來進行犯罪,而且兩岸華人都相繼傳出案例。比如2007年中國浙江省也有一名男子利用木馬病毒,遙控一名美女在電腦架設的網路攝影機鏡頭(webcam),拍下她脫衣服影片。這名男子食髓知味竟把影片裸照回傳給這名女子,要求她再脫一次。最後女子報警,這位半年內入侵百部電腦的男子終於被警方逮捕。在這個案例中,駭客遙控偷拍過程如下:

1. 在特定網頁上植入木馬
2. 受害者點選特定網頁後中毒但不自知
3. 駭客遙控受害者的網路攝影機並錄下裸照影片



案例5-分析

- 主要資產：
 - 業務流程和活動：個人電腦使用
 - 資訊：視電腦用途而定
- 支援資產：
 - 人員
 - 軟體
 - 網路

案例5-分析



- 風險擁有者(risk owners)：資安長/隱私長
- 風險：機密性—個資外洩
- 對應之ISO 27001:2013控制措施
 - A.7.2.2 Information security awareness, education and training 資訊安全認知、教育及訓練
 - A.8.1.3 Acceptable use of assets 資產之可被接受的使用

案例5-分析



- A.12.2.1 Controls against malware
對抗惡意軟體的控制措施
- A.12.6.1 Management of technical vulnerabilities 技術脆弱性管理
- A.12.6.2 Restrictions on software installation
限制軟體安裝
- A.18.2.2 Compliance with security policies and standards 安全政策與標準的遵循性





個資保護風險管理

個資法律法規的相關要求

個人資料保護法

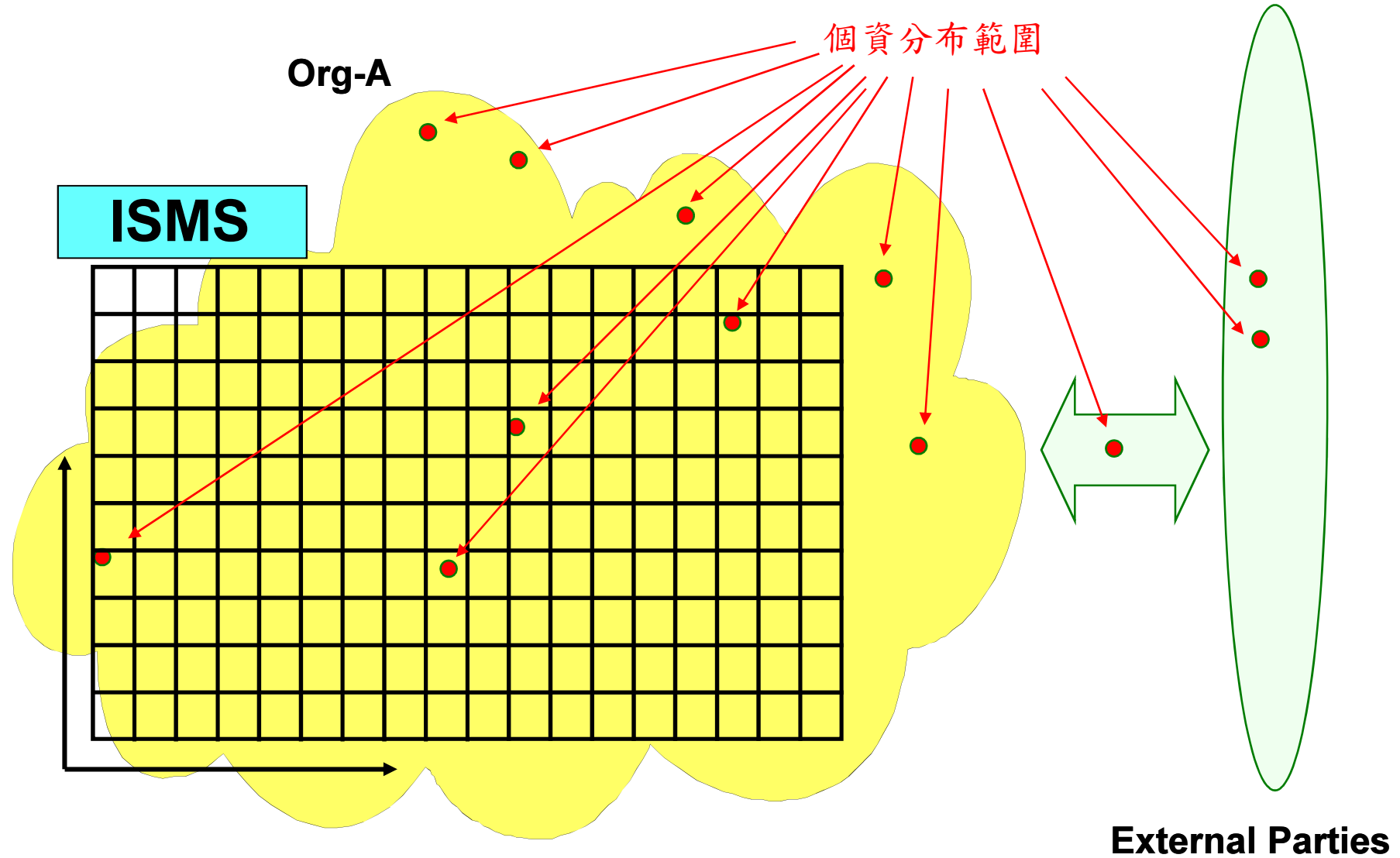
第28條 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

第29條 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。

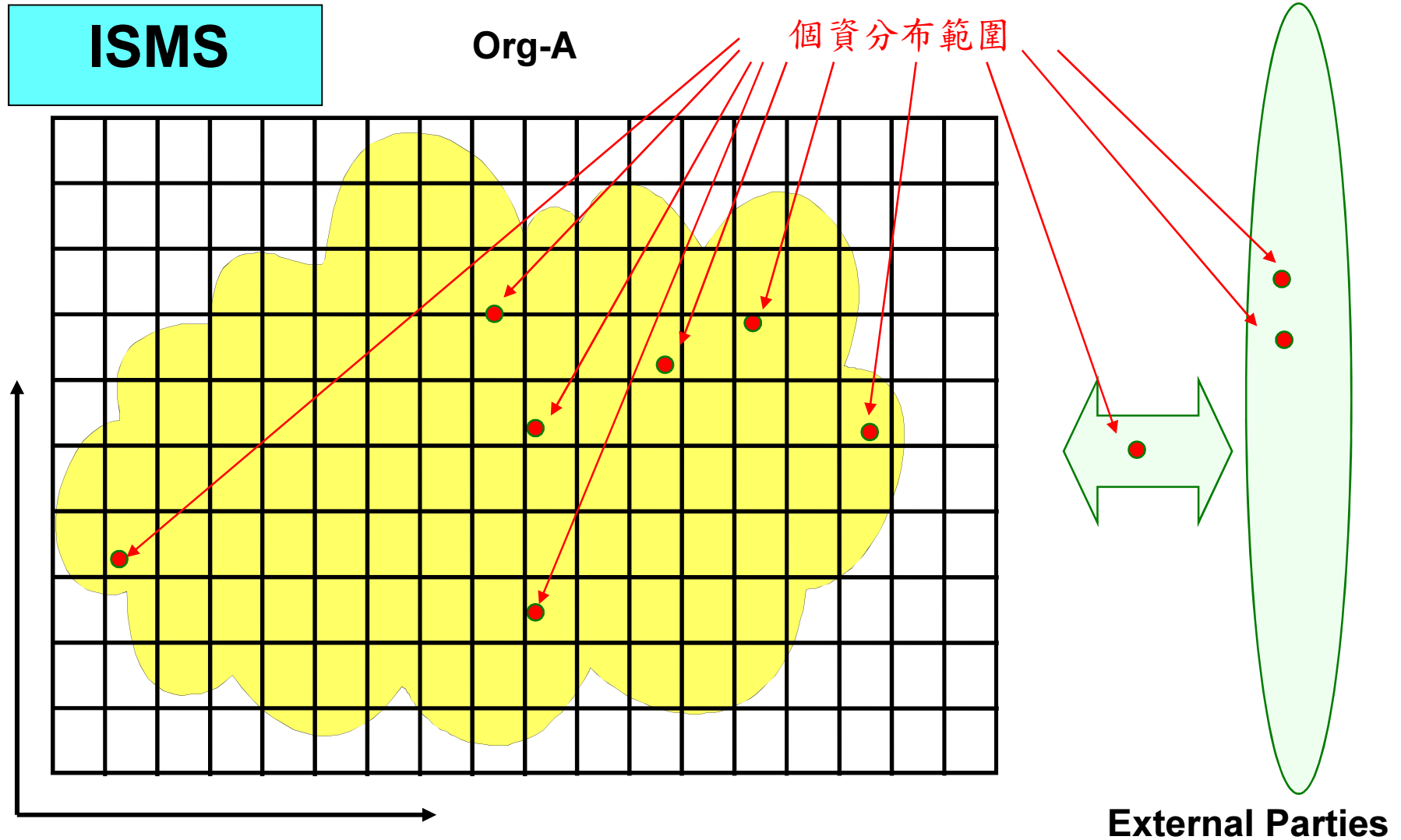
個資法相關要求 VS 組織的良善管理



個資分布範圍與管理系統範圍-1



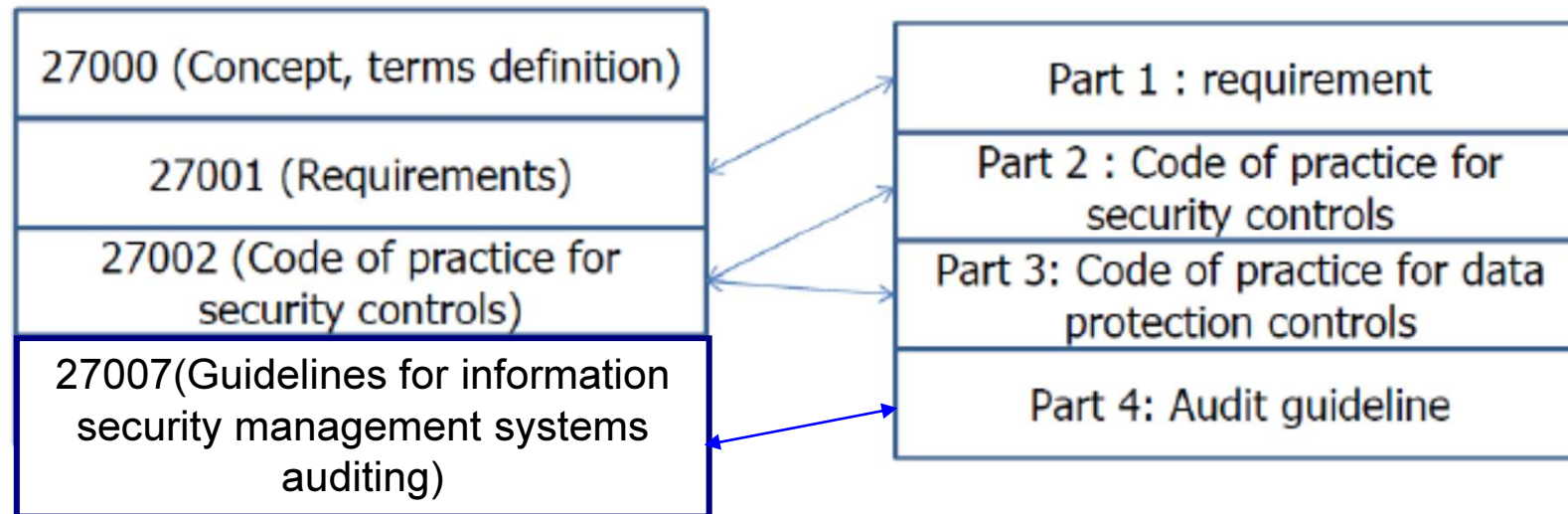
個資分布範圍與管理系統範圍-2



ISO組織發展中的個資管理系統(PIMS)



個資管理系統(PIMS)



multiple standards

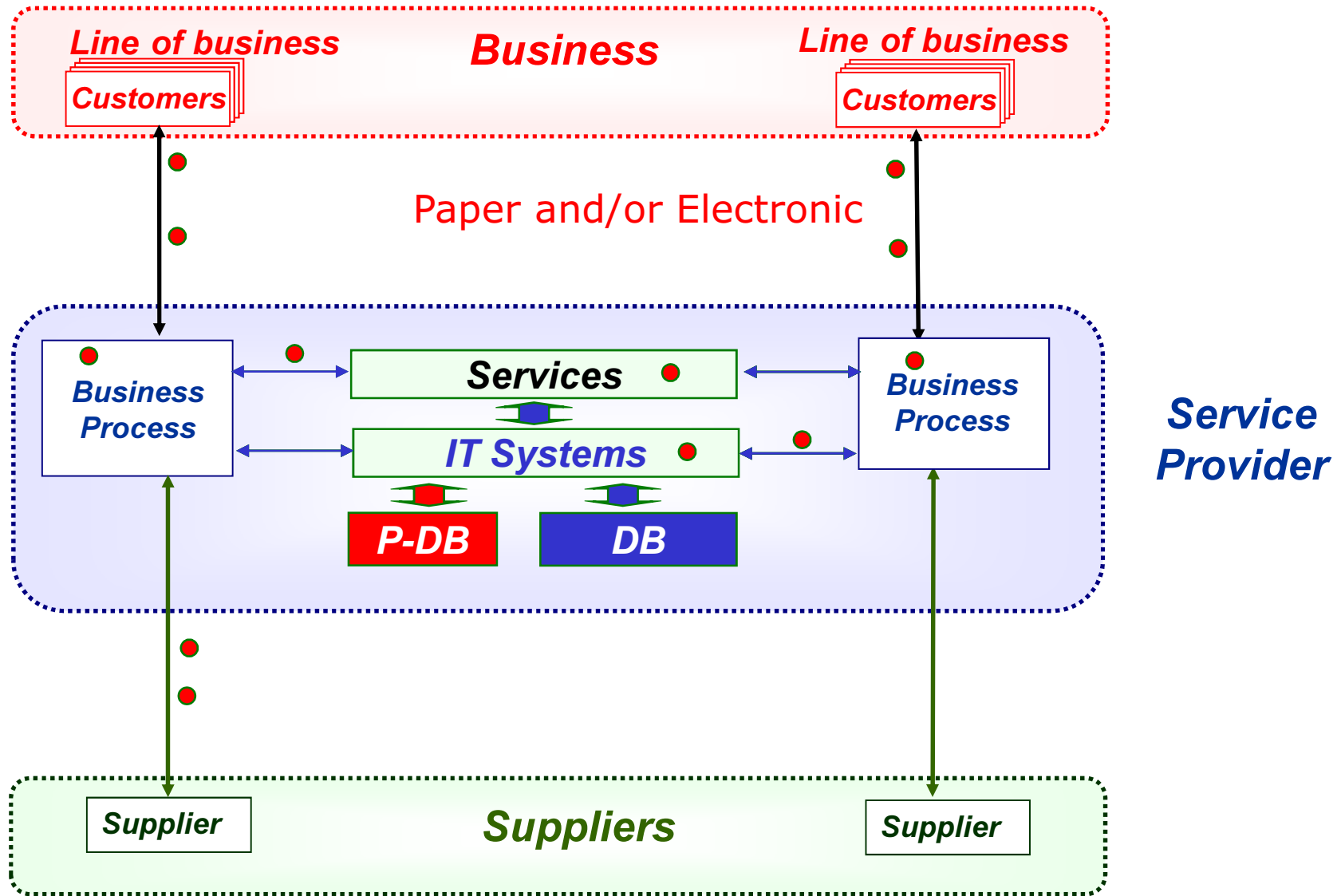
- ✓ ISO/IEC 27xxx Requirements for personal information management system
- ✓ ISO/IEC 27xxx Code of practice for security controls for personal information management
- ✓ ISO/IEC 29xxx Code of practice of data protection controls for the personal information management
- ✓ ISO/IEC 27xxx Auditing guidelines for the personal information management

資料/參考來源：

- ✓ ISO/IEC JTC 1/SC 27的WG1與WG5
- ✓ Heung Youl Youm (2011) Personal information management system in Korea (Presentation), RAISE 2011 in Seoul, 2011-11-24。

個人資料之風險評估及管理機制(例)

Facing The Law (個資法)



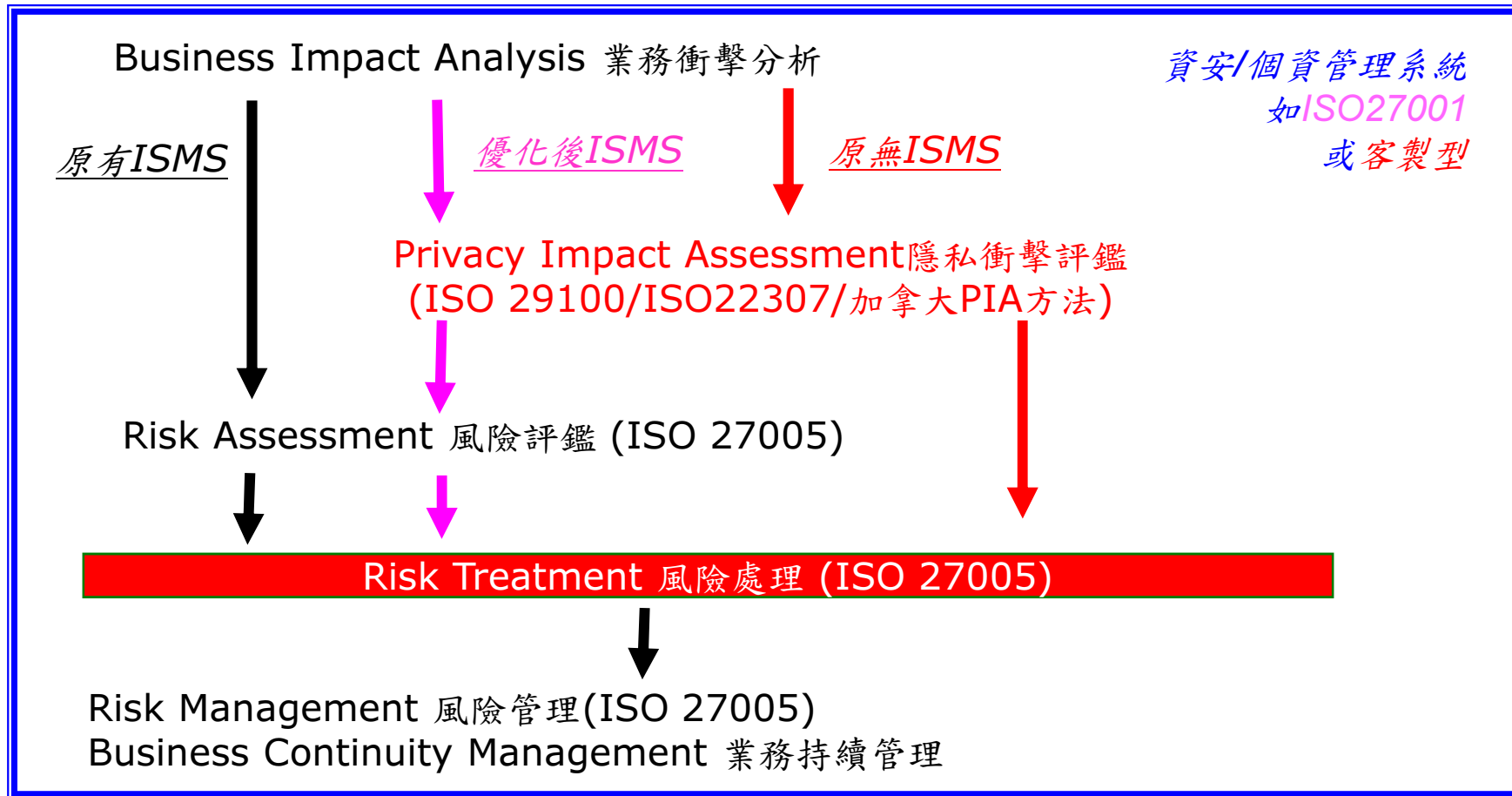
個人資料之風險評估及管理機制(例)



資安/個資風險管理的可能路徑

若原已有ISO27001：由黑線優化到粉紅線

若原無ISMS或ISO27001：直接進行紅線



良善管理的展現: 獨立第三方的ISO27001驗證、資安/個資遵循性評鑑



個人資料之風險評估及管理機制(例)



個資保護與國際標準關係參考圖

資安與個資管理(黑色粗線): ISO27001/ISO27002及特定產業適用標準, 如: 醫療ISO27799

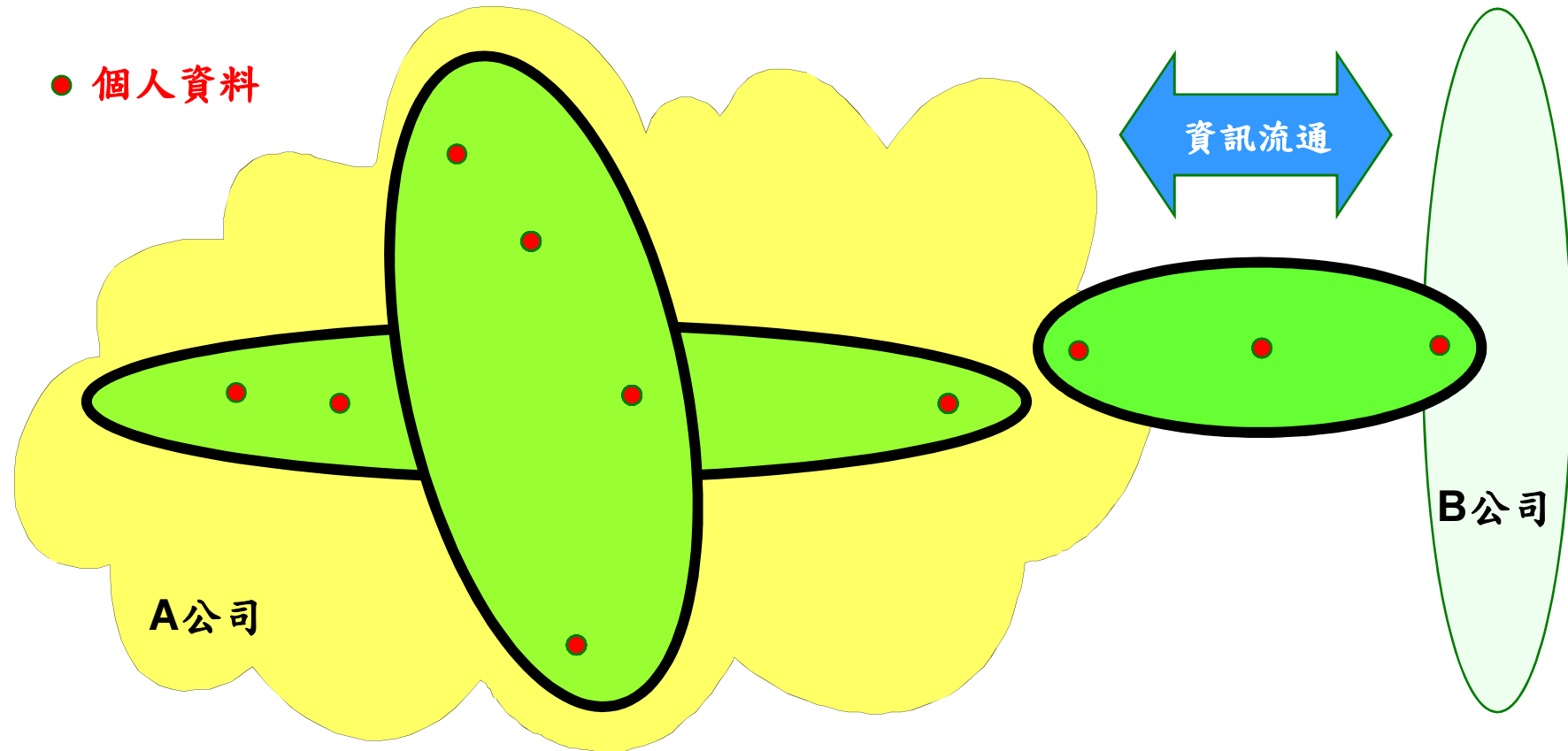
個資風險管理(綠色區域): ISO27005/ISO29100

隱私衝擊評鑑(PIA, 紅色點狀): ISO22307/加拿大PIA方法

跨公司資訊流通(藍色區域): ISO27010

良善管理的展現: 獨立第三方的ISO27001驗證/個資遵循性評鑑

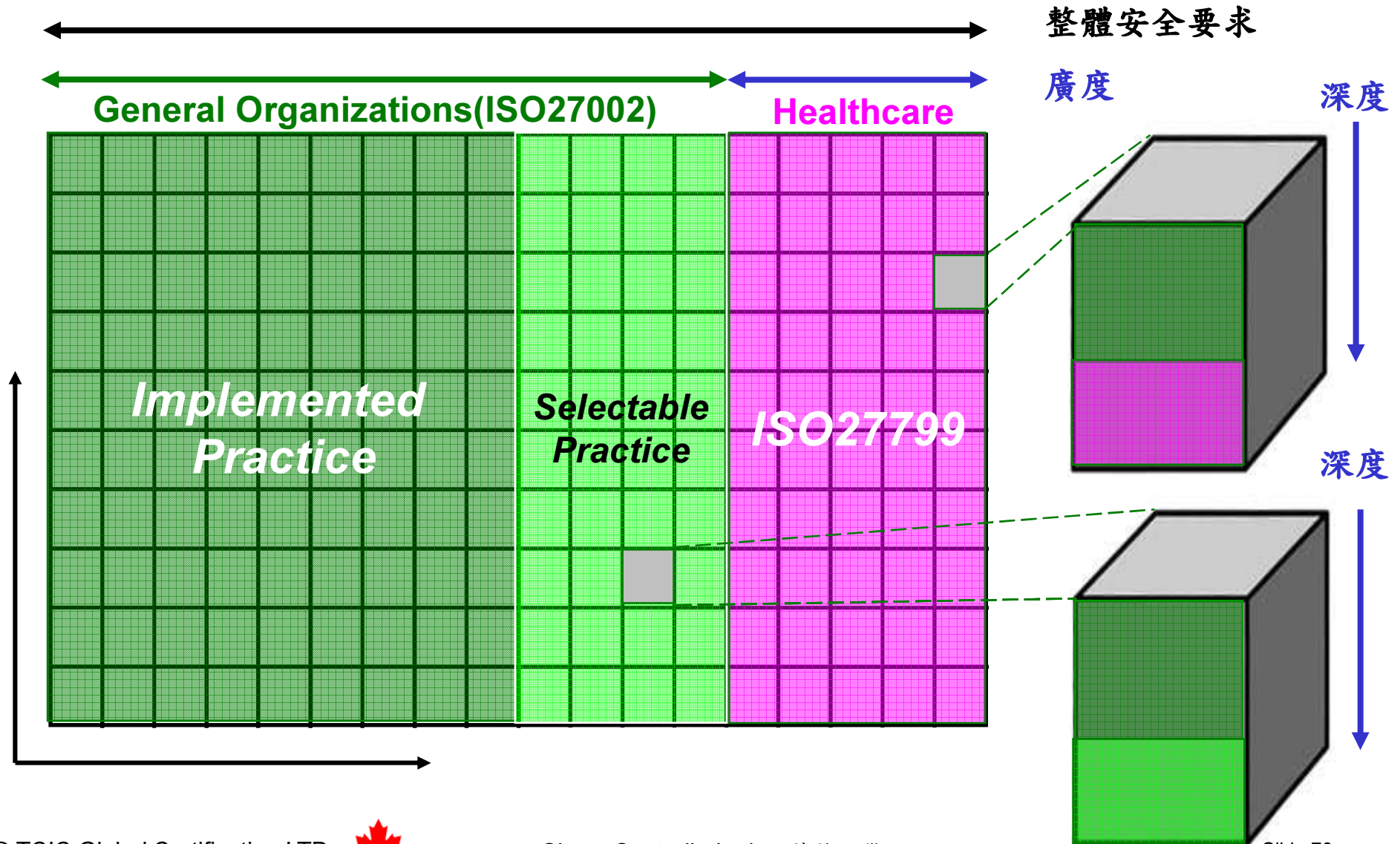
● 個人資料



個人資料之風險評估及管理機制(例)



The relationships between ISO27799 and ISO27001/ISO27002



整體安全要求

廣度

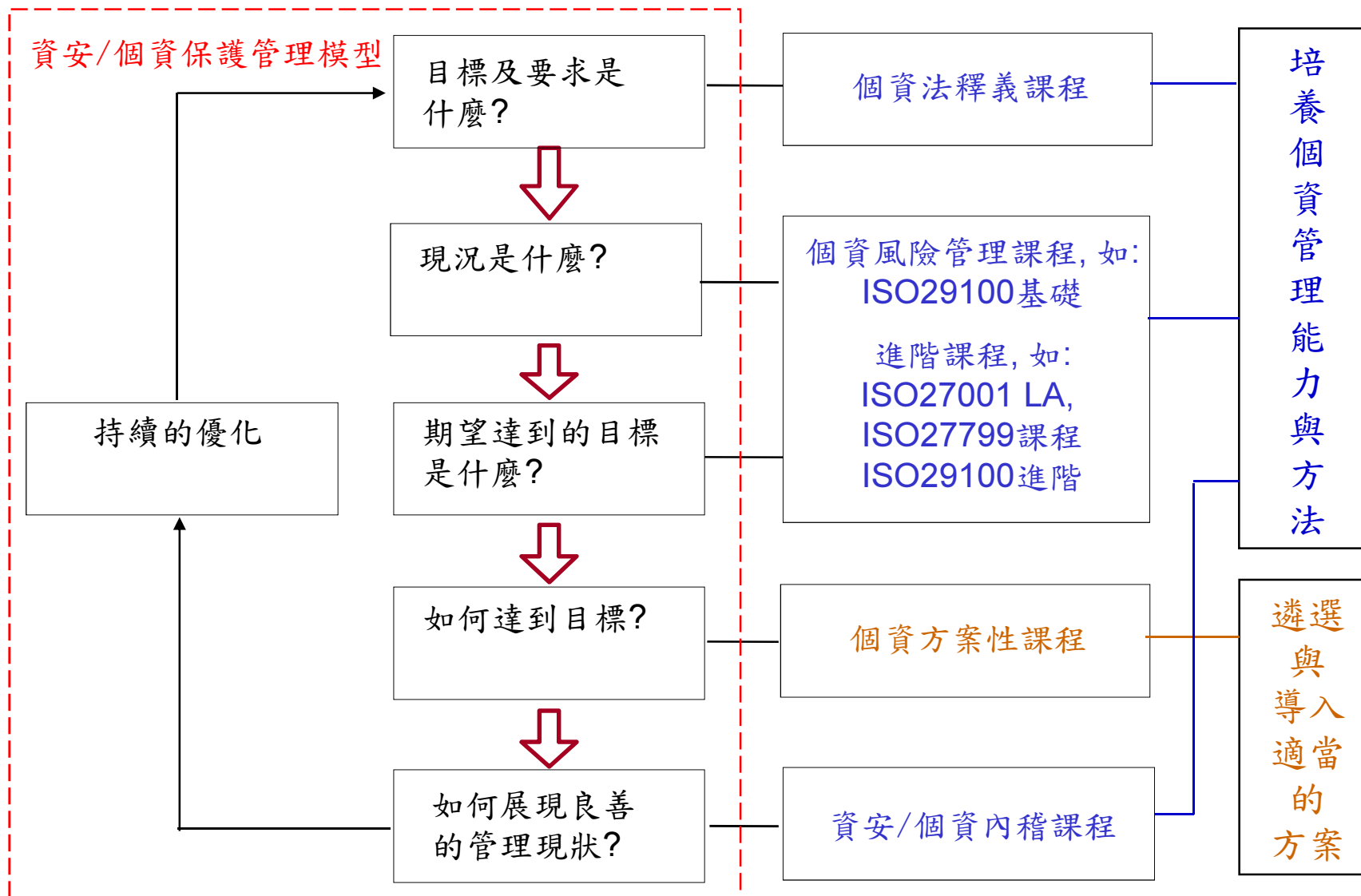
深度

深度

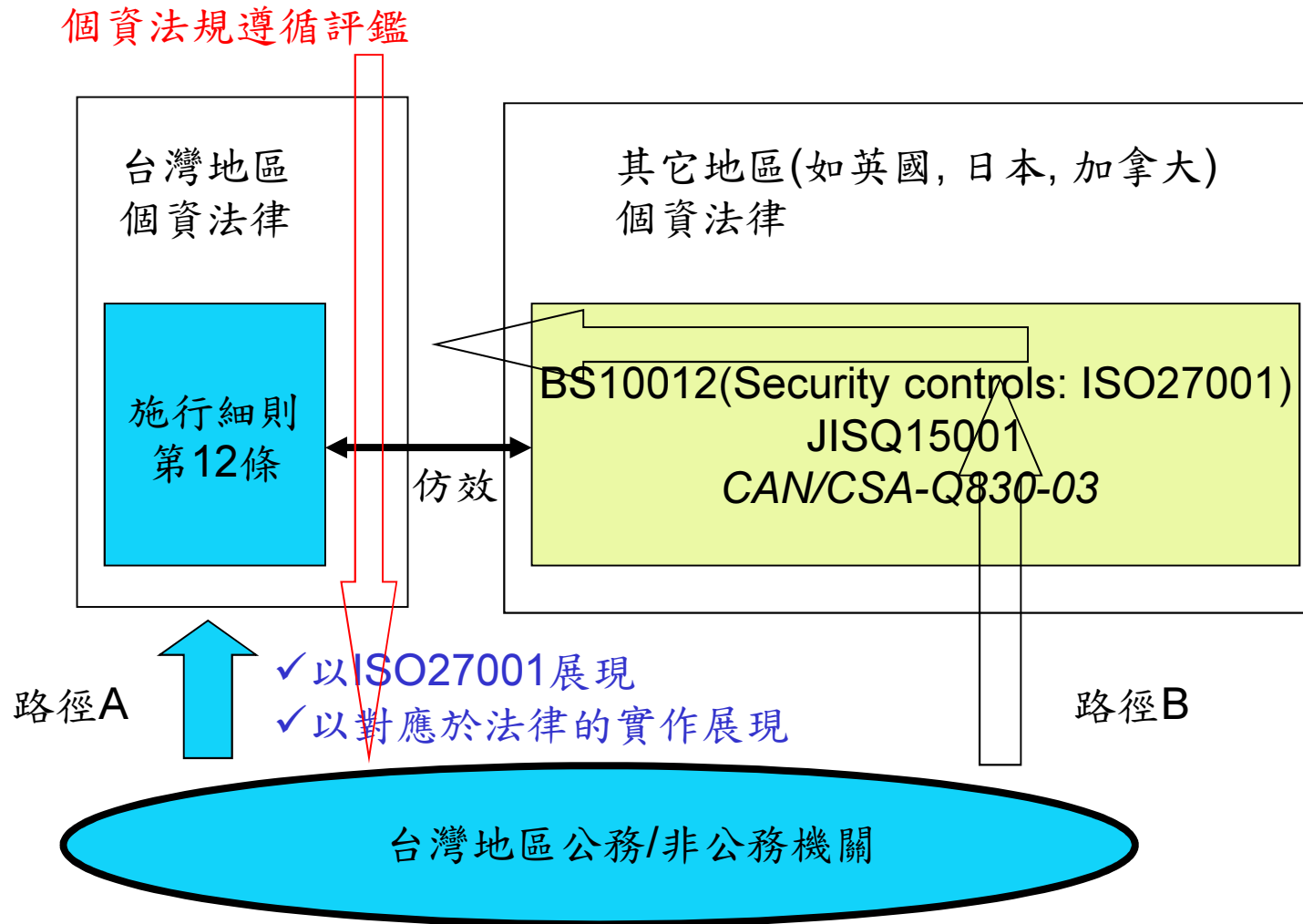


個資保護學習分布圖

認知宣導及教育訓練



選擇適當的方法以展現良善管理



考量對組織最有利的展現, 選擇最佳的展現方法.

Any questions ?



Thank you • Merci

For further information or enquiries, please contact :

Ms. Angel Hsu 許毓如, Service Coordinator

Email: angel@mail.tcicgroup.com , TEL: 02-27260262 Ext.121, FAX: 02-27260663