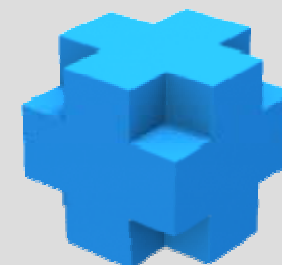




ISO 27001 資訊安全簡介

講師：黃金月

日期：99年11月11日



課程大綱

1. 資訊安全概觀

2. 資訊安全管理制度沿革

3. 資訊安全管理制度介紹

4. 重視個資與隱私保護

5. 問題與討論



1. 資訊安全概觀

2. 資訊安全管理制度沿革

3. 資訊安全管理制度介紹

4. 重視個資與隱私保護

5. 問題與討論

資訊的型式

- ❖ 以紙本書面的方式呈現，例如圖書、報紙、雜誌、作業、報表、廣告宣傳單等。
- ❖ 以電子方式儲存，例如磁碟、磁帶、光碟、隨身碟、影帶、影碟、記憶體等。
- ❖ 以無形的方式存在，例如知名度、形象、品牌、記憶等。
- ❖ 有形的實體物，例如商標等。



資訊的安全

- ❖ 有價值的資訊，需有適當的保護與使用控管，才能落實其真正的價值。
- ❖ 資訊安全的意義就是保護資訊，使資訊免於受到破壞，影響其使用。



資訊安全三大原則

❖ 機密性(Confidentiality)

- 確保資訊只有獲得授權的人才能存取。

❖ 完整性(Integrity)

- 確保資訊在維護與處理過程中沒有遭到變動與竄改。

❖ 可用性(Availability)

- 確保經授權的使用者在需要時，可以適時取得資訊。

資訊安全問題可能發生在……

❖ 傳送

- 資訊透過網路或儲存媒體由一處移至他處的過程，過程中資訊可能遭到竄改或盜取。

❖ 設備

- 儲存媒體或處理資訊的軟硬體系統，可能受到破壞。

❖ 資訊環境

- 提供資訊設備運轉以及保護資訊設備的外在資源，例如機房、電力、空調、網路連線的失效。

❖ 人員

- 未俱備認知或操作錯誤等。

常見的資訊安全威脅

- ❖ 天然災害造成業務中斷。
- ❖ 駭客入侵與惡意程式。
- ❖ 人員疏失、操作不當造成的損害。
- ❖ 惡意的內部人為破壞。
- ❖ 資料毀損或外洩。
- ❖ **違反法令法規。**





1. 資訊安全概觀

2. 資訊安全管理制度沿革

3. 資訊安全管理制度介紹

4. 重視個資與隱私保護

5. 問題與討論

何謂ISMS

- ❖ ISMS (Information security management system)
- ❖ 稱為「資訊安全管理系統」或「資訊安全管理
制度」：乃組織整體管理制度的一部份，必需依
據風險管理的方法加以制訂，進而用以建立、執
行、操作、監控、審查、維護與改進組織的資訊
安全。
 - ISMS目的在於保護資訊資產的機密性、可用性與完整
性。

何謂ISO 27001

- ❖ 為目前國際上最廣泛採用之資訊安全管理制度標準規範，為建立完善之資訊安全管理制度提供一個良好的起點及系統化的方法。
- ❖ 資訊安全管理制度標準規範中，絕大部份著重的是在於管理面的要求，其次才是技術面的專業知識。
- ❖ 此制度標準規範提醒在建構及管理整個制度面時，所須留意且不可忽略的層面，並藉由審查機制、事件的回饋及內部稽核，以預防資訊安全事件的或是降低損失的風險。

資訊安全管理制度的歷史沿革

1992	世界經濟開發組織(OECD)：資訊系統安全指導方針
1993	率先由英國貿易工業部進行專案
1995	英國公佈BS 7799 Part 1、Part 2
1999	新版英國標準 BS 7799 Part 1 & Part 2發行
2000	提交ISO組織討論；12月正式成為ISO 17799標準
2002	9月正式公佈BS 7799-2: 2002
2005	改版ISO 17799:2005；發行ISO 27001:2005
2007	ISO/IEC 17799作業規範，正名為ISO 27002
2009	ISO/13335，正名為ISO 27005





1. 資訊安全概觀

2. 資訊安全管理制度沿革

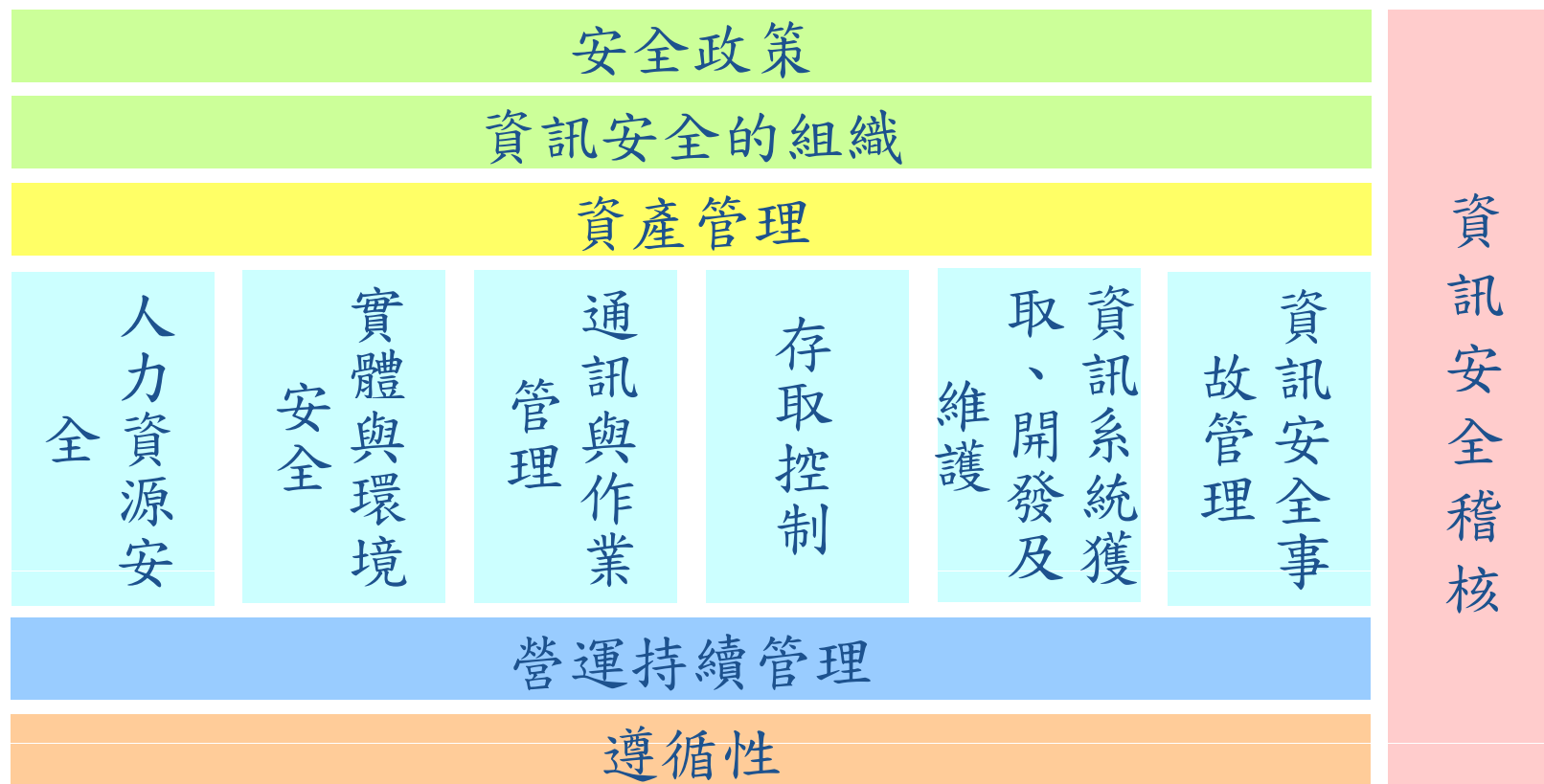
3. 資訊安全管理制度介紹

4. 重視個資與隱私保護

5. 問題與討論

ISO 27001涵蓋之內容

❖ 11 個管理領域、39 個控制目標、133 個控制要點。



- ❖ 定義高階管理對資訊安全之期許與要求，並將其文件化，以利組織內資訊安全之推行
 - 組織是否訂有資訊安全政策？
 - 組織之資訊安全政策文件是否由**管理階層**核准並**正式發布且轉知所有員工**？
 - 是否指定**專人或專責單位**進行資訊安全政策維護及檢討？
(同個人資料保護法第18條-專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。)



資訊安全的組織

❖ 成立資訊安全組織，並定義其組織架構、運作流程與責任歸屬

- 是否指定高級主管人員或成立跨單位組織負責推動、協調監督及審查資訊安全管理事項？
- 是否訂定規範員工的資訊安全作業程序與權責(含經管使用設備及作業須知)？
- 委外契約中是否包含法律需求(如個人資料保護法)、界定雙方有關人員權責、使用何種實體與邏輯安全控管措施、對委外廠商稽核權、得依實際需要可修改安全控制措施及作業程序等條文？

- ❖ 依照資訊資產之運作流程與資產價值，將資訊資產作分類，並規劃各不同等級資產所需之保護措施
 - 資產是否列有清冊，並加以維護？
 - 是否訂有資訊分級標示與處理之相關規範？
 - 資產是否予以分級並作標示處理？

❖ 降低人為疏失發生機率，並減少人為之惡意侵害行為

- 針對人員之調動、離職或退休，是否立即取消其各項識別碼、通行碼？
- 員工是否瞭解單位之資訊安全政策及應負之責任？
- 員工(含第三方使用者)是否依職務層級進行適當的資訊安全教育訓練？
- 下班後員工是否將經辦之機密性資料，妥善收藏？

❖ 規範有形資產之保護措施、安全裝備、與一般控管原則

- 個人電腦及終端機不使用時是否關機、登出，或設定有密碼之螢幕保護程式或其他控制措施進行保護？
- 對於資訊財產攜出辦公處所，是否訂有攜出管理規則(含安全查核)？
- 在組織場所以外使用資訊設備或存取資料是否訂有安全保護措施？
- 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？

❖ 確保通訊、資訊設備的作業處理之安全性

- 日常作業是否有文件化的操作程序？
- 網路服務是否有安全的管理措施？
- 機密性資料之儲存或處理是否有安全處理程序？
- 對外開放之資訊，是否訂有保護措施以確保資訊完整性？
- 未經授權的活動是否予以監控？

- ❖ 使用者權限之設定應依使用者工作職權而給予，以降低未經授權存取系統資源之風險
 - 是否訂有資訊存取控制政策及相關說明文件？
 - 使用者存取權限是否定期檢查，或在權限變更後立即複檢？
 - 遠距工作是否得到管理階層授權並執行必要之保護措施？
 - 系統存取及特別權限的配置使用情形是否予以監控？



資訊系統獲取、開發及維護

❖ 規劃組織內系統開發與維護過程，將資訊安全控管列入流程範圍

- 應用系統在規劃分析時是否將安全需求納入分析及規格？
- 應用系統上線前是否經測試？
- 對高敏感性的資料在傳輸或儲存中是否使用加密技術？
- 是否建立應用系統之變更管制程序？
- 是否執行原始碼版本控管？
- 原始程式庫之存取行為，是否留有稽核日誌？



資訊安全事故管理

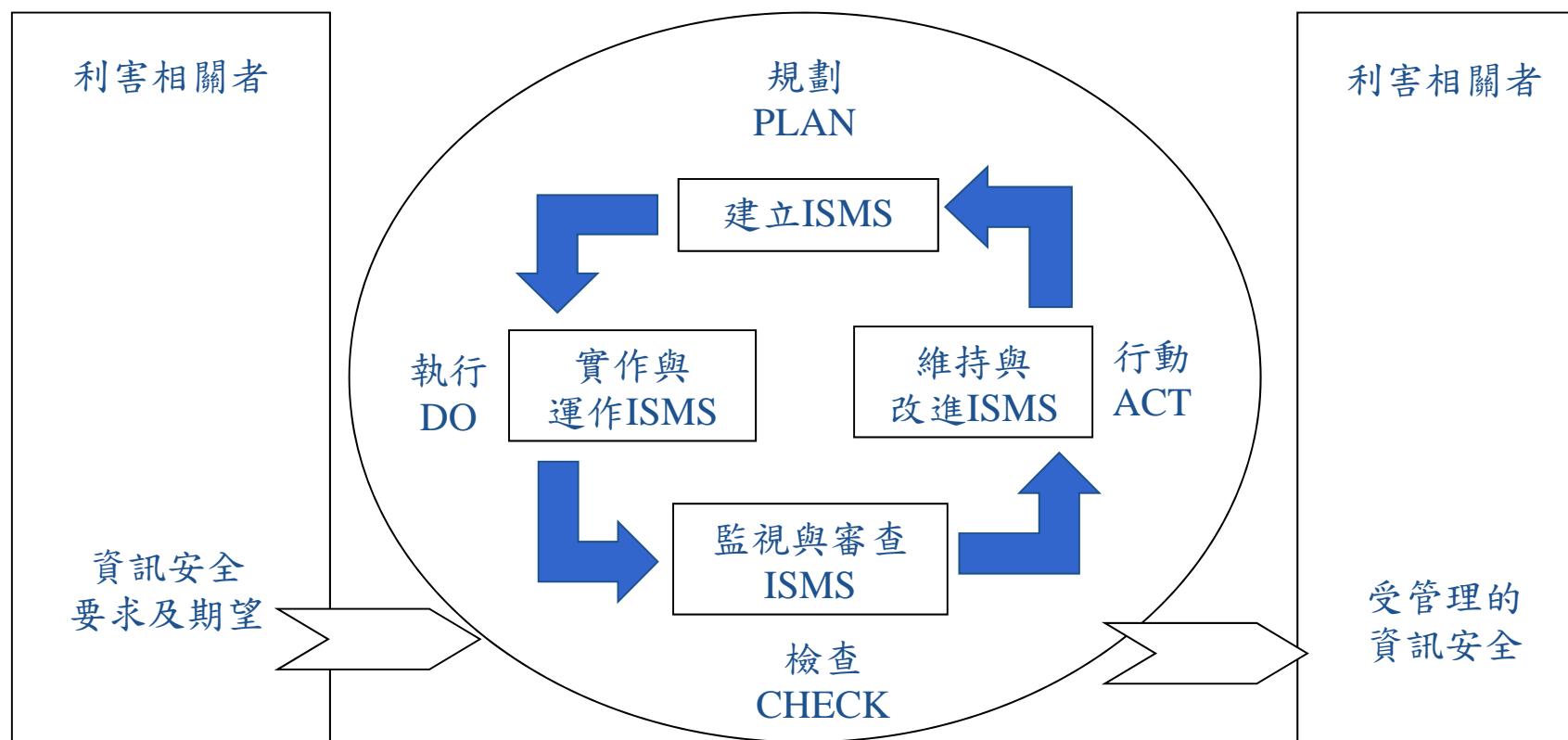
- ❖ 確保資訊安全事件能以適當方式在組織內傳遞，並得以及時採取適當應變方案
 - 是否已擬訂資訊安全事件通報程序？
 - 是否適當管理相關資訊安全事件？

- ❖ 針對各種可能的意外災害，研擬適當應變方案，以確保業務得以持續運作
 - 是否已擬訂關鍵性業務及其衝擊影響分析？
 - 是否擬訂營運持續計畫？
 - 營運持續計畫是否定期測試演練？
 - 營運持續計畫是否定期審查和更新？

- ❖ 各種法規，如電子簽章法、個人資料保護法...等
相關法規及組織資訊安全政策之遵循
 - 組織中對於所經營或處理之資訊，涉有個人隱私及個人資料之保護是否有妥適之保護機制？
 - 是否安裝合法授權軟體？
 - 是否定期辦理資訊安全內部稽核？
 - 是否訂有資訊安全內部稽核計畫
 - 稽核後是否產生稽核報告並追蹤改善情形(包括稽核發現的摘要、稽核區域、缺失說明及改進建議等)？

資訊安全管理制度架構

❖ 過程導向(作法)(process approach)



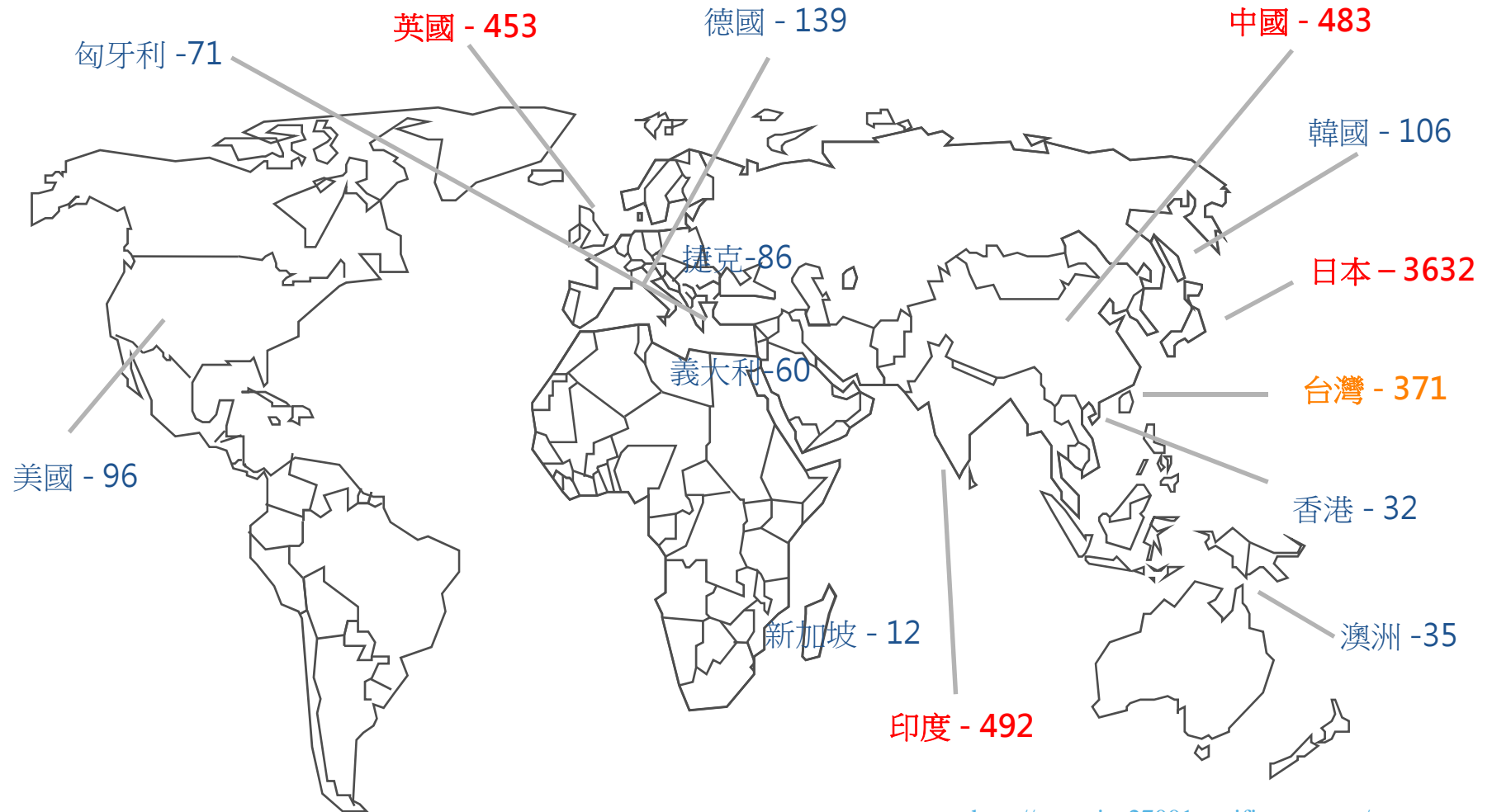
資訊安全管理制PDCA

規畫 (建立ISMS)	建立與管理風險及改進資訊安全相關之ISMS的政策、目標、過程及程序以產生與組織整體政策和目標相一致之結果。
執行(實作與運作ISMS)	實作與運作ISMS的政策、控制措施、過程及程序。
檢查(監視與審查ISMS)	依據ISMS政策、目標及實際經驗，評鑑及在適用時測量過程績效，並將結果回報給管理階層審查。
行動(維持與改進ISMS)	基於ISMS內部稽核與管理階層審查結果或其它相關資訊採取矯正與預防措施，以達成ISMS的持續改進。

資訊安全管理制度趨勢

- ❖ 在政府帶動下，許多電信、金融、教育單位與資訊服務，為能取得客戶信任、保護重要資訊資產，紛紛推動ISMS的建置ISMS（Information security management system）。
- ❖ 在法規要求以及客戶期望下，推行資訊安全管理制度已成為組織永續經營之必要工作。

ISO 27001全球推廣狀況



<http://www.iso27001certificates.com/>
As of 2010/10





ISO 27001全球推廣狀況~1

Japan	3632	Philippines	15	Macau	3
India	492	Pakistan	14	Portugal	3
China	483	Vietnam	14	Argentina	2
UK	453	Iceland	13	Belgium	2
Taiwan	371	Saudi Arabia	13	Bosnia Herzegovina	2
Germany	139	Netherlands	12	Cyprus	2
Korea	106	Singapore	12	Isle of Man	2
USA	96	Indonesia	11	Kazakhstan	2
Czech Republic	86	Bulgaria	10	Morocco	2
Hungary	71	Kuwait	10	Ukraine	2
Italy	60	Norway	10	Armenia	1
Poland	56	Russian Federation	10	Bangladesh	1
Spain	54	Sweden	9	Belarus	1
Malaysia	40	Colombia	8	Denmark	1
Ireland	37	Bahrain	7	Dominican Republic	1
Thailand	36	Iran	7	Jersey	1
Austria	35	Switzerland	7	Kyrgyzstan	1
Hong Kong	32	Canada	6	Lebanon	1
Greece	30	Croatia	6	Luxembourg	1
Romania	30	South Africa	5	Macedonia	1
Australia	29	Sri Lanka	5	Mauritius	1
Mexico	24	Lithuania	4	Moldova	1
Brazil	23	Oman	4	New Zealand	1
Slovakia	21	Peru	4	Sudan	1
Turkey	21	Qatar	4	Uruguay	1
UAE	20	Chile	3	Yemen	1
France	19	Egypt	3		
Slovenia	17	Gibraltar	3		
			30	Total	6826

<http://www.iso27001certificates.com/>
As of 2010/10

學校單位推動狀況-B級

序號	學校名稱	ISO 27001	教育版	建置中
1	國立政治大學		V	
2	國立清華大學		V	
3	國立台灣大學		V	
4	國立台灣師範大學			V
5	國立成功大學		V	
6	國立中興大學		V	
7	國立交通大學	V	V	
8	國立中央大學	V	換	
9	國立中山大學		V	
10	國立台灣海洋大學			
11	國立中正大學		V	
12	國立高雄師範大學			
13	國立彰化師範大學		V	
14	國立陽明大學	V		
15	國立台北大學			V
16	國立嘉義大學		V	
17	國立高雄大學		V	
18	國立東華大學		V	
19	國立暨南國際大學			V
20	國立台灣科技大學			V
21	國立雲林科技大學		V	
22	國立屏東科技大學	V		

序號	學校名稱	ISO 27001	教育版	建置中
23	國立台北科技大學		V	
24	國立高雄第一科技大學	V	V	
25	國立高雄應用科技大學			
26	國立台北藝術大學			V
27	國立台灣藝術大學			V
28	國立台東大學		V	
29	國立宜蘭大學		V	
30	國立聯合大學		V	
31	國立虎尾科技大學		V	
32	國立高雄海洋科技大學	V	換	
33	國立台南藝術大學			
34	國立台南大學			V
35	國立台北教育大學			V
36	國立新竹教育大學		V	
37	國立台中教育大學			V
38	國立屏東教育大學		V	
39	國立澎湖科技大學			
40	國立勤益科技大學	V		
41	國立體育大學			
42	東海大學	V		
43	輔仁大學	V		
44	東吳大學	V		

學校單位推動狀況-B級(續)

序號	學校名稱	ISO 27001	教育版	建置中
45	中原大學	V		
46	淡江大學	V		
47	中國文化大學	V	換	
48	逢甲大學	V		
49	靜宜大學	V	換	
50	長庚大學	V		
51	元智大學	V		
52	中華大學		V	
53	大葉大學	V		
54	華梵大學		V	
55	義守大學	V		
56	世新大學	V	換	
57	銘傳大學	V		
58	實踐大學	V		
59	朝陽科技大學	V		
60	高雄醫學大學		V	
61	南華大學			V
62	真理大學		V	
63	大同大學	V		
64	南臺科技大學	V	換	
65	崑山科技大學	V		
66	嘉南藥理科技大學	V		

序號	學校名稱	ISO 27001	教育版	建置中
67	樹德科技大學	V		
68	慈濟大學		V	
69	台北醫學大學	V		
70	中山醫學大學		V	
71	龍華科技大學	V	換	
72	輔英科技大學	V	換	
73	明新科技大學	V	V	
74	長榮大學		V	
75	弘光科技大學	V	換	
76	中國醫藥大學	V		
77	清雲科技大學	V	換	
78	正修科技大學		V	
79	萬能科技大學		V	
80	玄奘大學		V	
81	建國科技大學	V		
82	明志科技大學	V		
83	高苑科技大學		V	
84	大仁科技大學			
85	聖約翰科技大學			
86	嶺東科技大學		V	
87	中國科技大學	V	換	
88	中臺科技大學			V

學校單位推動狀況-B級/C級

序號	學校名稱	ISO 27001	教育版	建置中
89	亞洲大學		V	
90	開南大學	V		
91	佛光大學		V	
92	台南應用科技大學			V
93	遠東科技大學		V	
94	元培科技大學		V	
95	景文科技大學	V		
96	中華醫事科技大學	V		
97	東南科技大學	V		
98	德明財經科技大學			
99	明道大學		V	
100	立德大學		V	
101	南開科技大學	V		
102	中華科技大學			
103	僑光科技大學			V
104	育達商業科技大學		V	
105	台北市立教育大學	V	換	
106	台灣首府大學		V	

序號	學校名稱	ISO 27001	教育版	建置中
2	國立台北護理學院	V		
4	國立台中技術學院	V	V	
14	文藻外語學院	V		
19	北台灣科學技術學院			V
21	醒吾技術學院	V		

❖ B級學校

- 通過ISO 27001-44單位
- 通過教育版-42單位
- 建置中-13個單位
- 未導入-10個單位

❖ C級學校

- 通過ISO 27001-4單位
- 通過教育版-1單位
- 建置中-1單位
- 未導入-52單位

資訊安全管理制度實施效益

- ❖ 提升組織競爭力與形象。
- ❖ 確保資訊之機密性、完整性與可用性。
- ❖ 降低資訊安全威脅。
- ❖ 建立資源管理機制。
- ❖ 建立管理程序。
- ❖ 確保業務持續運作。
- ❖ 強化風險管理。





1. 資訊安全概觀

2. 資訊安全管理制度沿革

3. 資訊安全管理制度介紹

4. 重視個資與隱私保護

5. 問題與討論

個資外洩嚴重

- ❖ 個資外洩讓個人、企業損失外，也造成治安上的問題。
- ❖ 內政部警政署165反詐騙專線於2009年統計
 - 購物資料外洩佔43%。
 - 網購未收到佔31%。
 - 假檢警詐騙為8%。
- ❖ 抱怨指數
 - 利用個資外洩為主要詐騙手法。
 - 電話及網路詐騙氾濫佔89.8%。



資料來源-內政部警政署、行政院研究發展考核委員會

重視個資與隱私保護

❖ 個人資料保護法

- 立法院於**99年4月27日**，將電腦處理個人資料保護法，修訂並三讀通過為「個人資料保護法」，**99年5月26日**經總統公布。
- **2012年1月**。

❖ 立法目的

- 第一條：為規範個人資料之**蒐集、處理及利用**，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

尋求個人資訊隱私權與資料合理流通之利益平衡。

個資法 名詞定義

❖ 蒐集

- 指以任何方式取得個人資料。

❖ 處理

- 指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

❖ 利用

- 指將蒐集之個人資料為處理以外之使用。

滿足處理的安全控管，落實 ISO 27001。

個資法重點摘要

❖ 範圍與主體普遍化

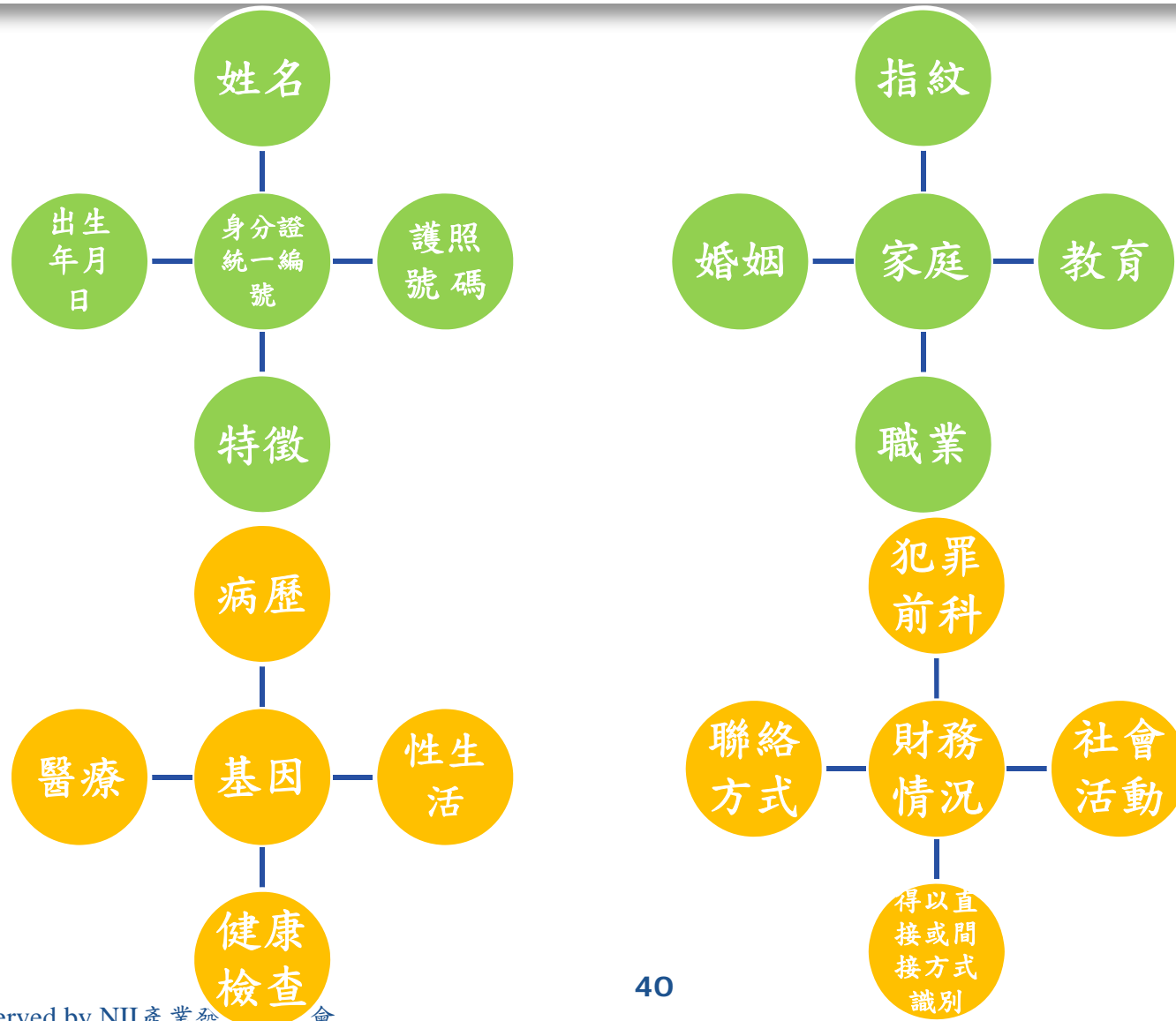
- 所有公民營機關，不限行業、自然人、法人或其他團體（含境外），全都納入規範。

❖ 不適用個資法之例外情形

- 自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。
- 對公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料

全面適用，包括你、我

個人資料之定義



個資法重點摘要

❖ 有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料不得蒐集、處理、利用，除非

- 法律明文規定。
- 當事人自行公開。
- 履行法定義務所必要，有適當安全控管。
- 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要且無從識別。

個資法重點摘要

❖ 強化行為規範

- 告知。
- 補行告知-施行日後一年內完成之告知義務。
- 書面同意。
- 拒絕機制。

❖ 團體訴訟

- 財團法人或公益社團法人經受有損害之當事人二十人以上以書面授權與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。

個資法重點摘要

❖ 違反個資法之刑事責任

- 違反蒐集以及利用之規定，或中央目的事業主管機關限制國際傳輸之命令或處分，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。(告訴乃論)
- 意圖營利犯前項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。(非告訴乃論)
- 意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。(告訴乃論但對公務機關犯本罪者為非告訴乃論)

個資法重點摘要

❖ 違反個資法之民事責任

■ 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。

■ 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。(第29條)

- 不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。

舉證責任，相對重要



個資法重點摘要

❖ 違反個資法之民事責任~1


- 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受前述每人每一事件最低賠償金額新臺幣五百元之限制。
- 損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。

舉證責任，相對重要

❖ 建立個資管理制度-展現良善管理

- 符合國家規範(如：ISO 27001，未來主管機關標章規範...)
- 符合國際規範
 - BS10012：2009-Personal Information Management System
 - JISQ 15000- Privacy Mark
 - APEC隱私權保護原則
 - ...
- 符合行業規範產業規範
 - 內控制度
 - PCI -Payment Card Industry
 - 產業規範

2009年6月2日



資料蒐集、處理、利用之自我檢查五步驟

步驟一：清點所有之個人資料



步驟二：清查蒐集個人資料之途徑與方式



步驟三：確認是否須履行告知義務並建立告知
機制



步驟四：確認蒐集、處理、利用之特定目的



步驟五：檢視利用的範圍與方式



問題與討論!

姓名：黃金月

e-mail：EmilyHuang@nii.org.tw

電話：(02)25082353 ext112

NII產業發展協進會

