資訊安全管理與個人資料保護

資訊風險管理組　　魯君禮 協理

財團法人中華民國國家資訊基本建設產業發展協進會

大綱

- 風險管理與資訊安全
- 個人資料保護

組織風險管理

資訊科技已經由組織基礎建設進化成為
不可或缺的**經營管理工具**

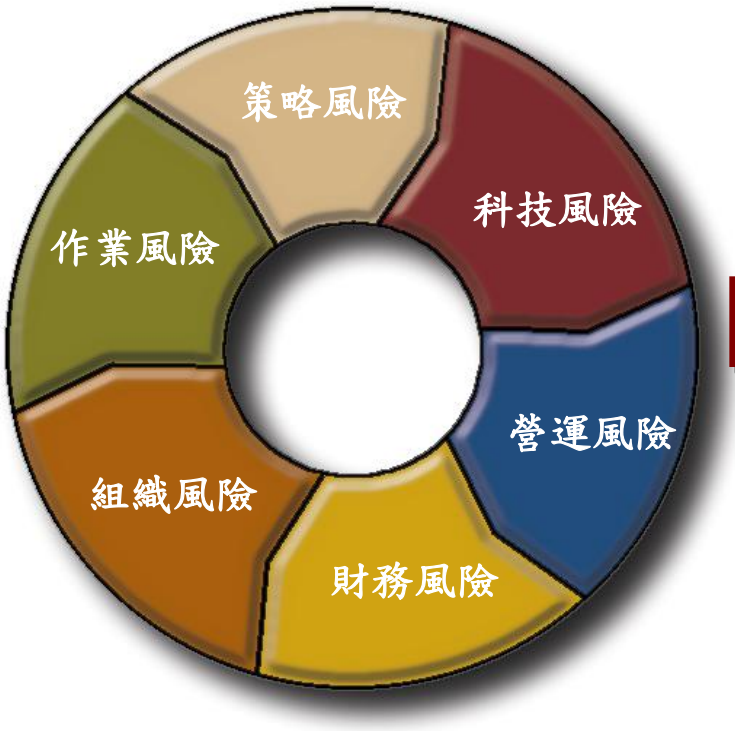
組織層級之管理

資訊科技(IT)

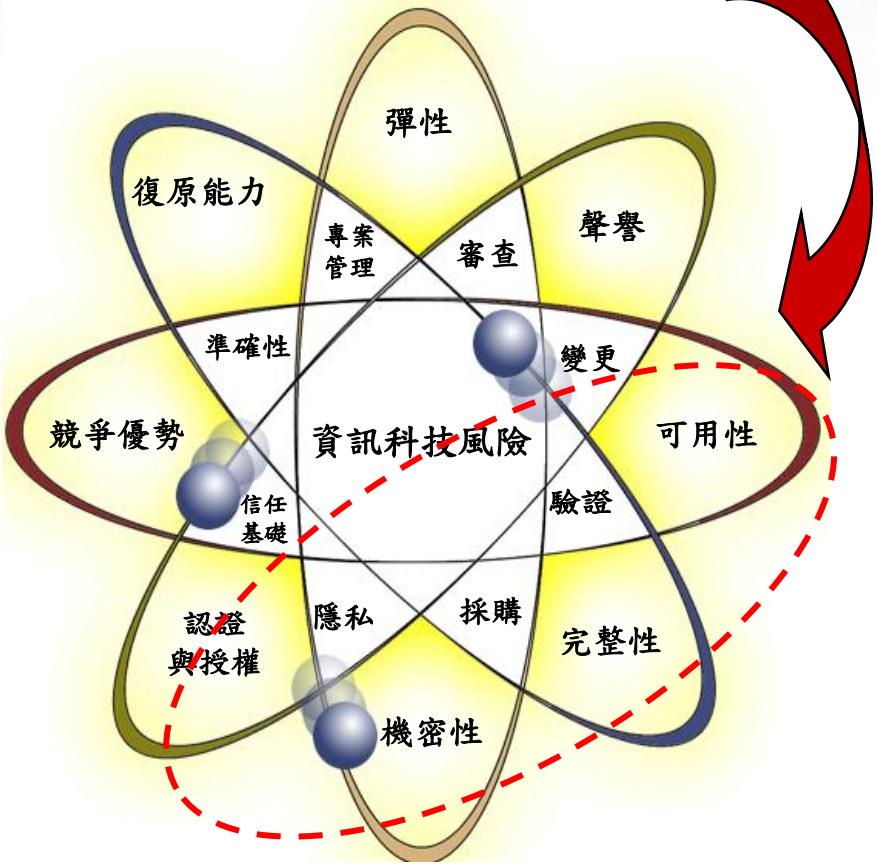
銷售及收款	採購及付款	生產	薪工
融資	固定資產	投資	研發

科技風險管理

資訊安全管理是科技風險管理的重要工作項目



執行力



資訊安全需求之來源

- 組織的業務需求(Business requirement)
  - ✓客戶的期望
  - ✓合作廠商的要求
- 法規的要求(Legal requirement)
  - ✓政府法令(電腦處理個人資料保護法、刑法、民法)
  - ✓主管機關規定(公開發行公司建立內部控制制度處理準則)
- 組織內部風險管理的需求(Risk control requirement)
  - ✓組織治理
  - ✓人力資源風險

資訊安全考量

- **機密性**（Confidentiality）
  - ✓ 確保涉及組織營運相關機密資訊只有經授權者可取得或揭露
- **完整性**（Integrity）
  - ✓ 確保重要資訊，在維護與處理過程保持其正確、完整且不受竄改。
- **可用性**（Availability）
  - ✓ 確保經授權的使用者在需要時可及時取得資訊。
- **可歸責性**（Accountability）
  - ✓ 確認某事件或行為可追溯至該行為或事件的承辦與負責人員或單位。
- **可靠性**（Reliability）
  - ✓ 確保相關重要資訊系統之穩定，並都能有預期之產出。

個人資料保護

國內外個資保護
現況及發展

國內

2007國際隱私權評比
台灣成績落後

2009電腦處理個人資料保護法
修法審議中

2008民意代表及團體建議政府
推動「隱私保護」認證制度

國外

2008經濟合作暨發展組織(OECD)
個人資料保護8大原則

2008亞太經濟合作組織強調
隱私權驗證機制及互信關係
跨境隱私規則國際執行領航者計畫

2008歐盟(EU)個人資料保護指令
保障個人自由、基本隱私權益及
確保個人資料自由流通

隱私權 or 個人資料保護

隱私權聲明範例：

- 隱私權保護政策的適用範圍
- 資料收集及使用方式
- 資料分享以及公開方式
- Cookies
- 修改個人帳號資料及偏好設定的權力
- 保全
- 隱私權保護政策修訂

隱私權=個人資料保護?

電腦處理個人資料保護法修訂草案

- 修法背景
- 法務部為因應急速變遷之社會環境，特別彙整國內學界與實務界的相關修法建議，並參考其他國家之個人資料保護相關法令來針對本法進行修訂
- 修訂草案共有55條，並將本法名稱修訂為「個人資料保護法」
- 草案修正方向
  - 擴大保護客體
  - 普遍適用主體
  - 增修行為規範
  - 強化行政監督
  - 妥適調整罰則
  - 促進民眾參與

電腦處理個人資料保護法修訂草案(續)

■ 修法重點說明

◆擴大保護客體：

- 為落實對個人資料之保護，將保護客體予以擴大，不再以經電腦處理個人之資料為限。

◆普遍適用主體：

- 刪除非公務機關行業之限制，使任何自然人及法人或其他團體，除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外，皆須適用本法。
- 公務機關及非公務機關，在中華民國領域外對中華民國人民蒐集、處理或利用個人資料者，亦有本法之適用。

◆調整責任內涵：

- 對於違法蒐集、處理或利用個人資料者，區別其是否具有「意圖營利」之主觀要件，科予程度不等之刑事責任。
- 為提昇法益保護之周延程度，中華民國人民在我國領域外觸犯本法之罪者，亦適用本法。
- 提高對非公務機關所課之罰緩額度；非公務機關之代表人、管理人或其他有代表權人，除能證明已盡防止義務者外，並應課以同一額度之罰緩，以加強其監督之責任。

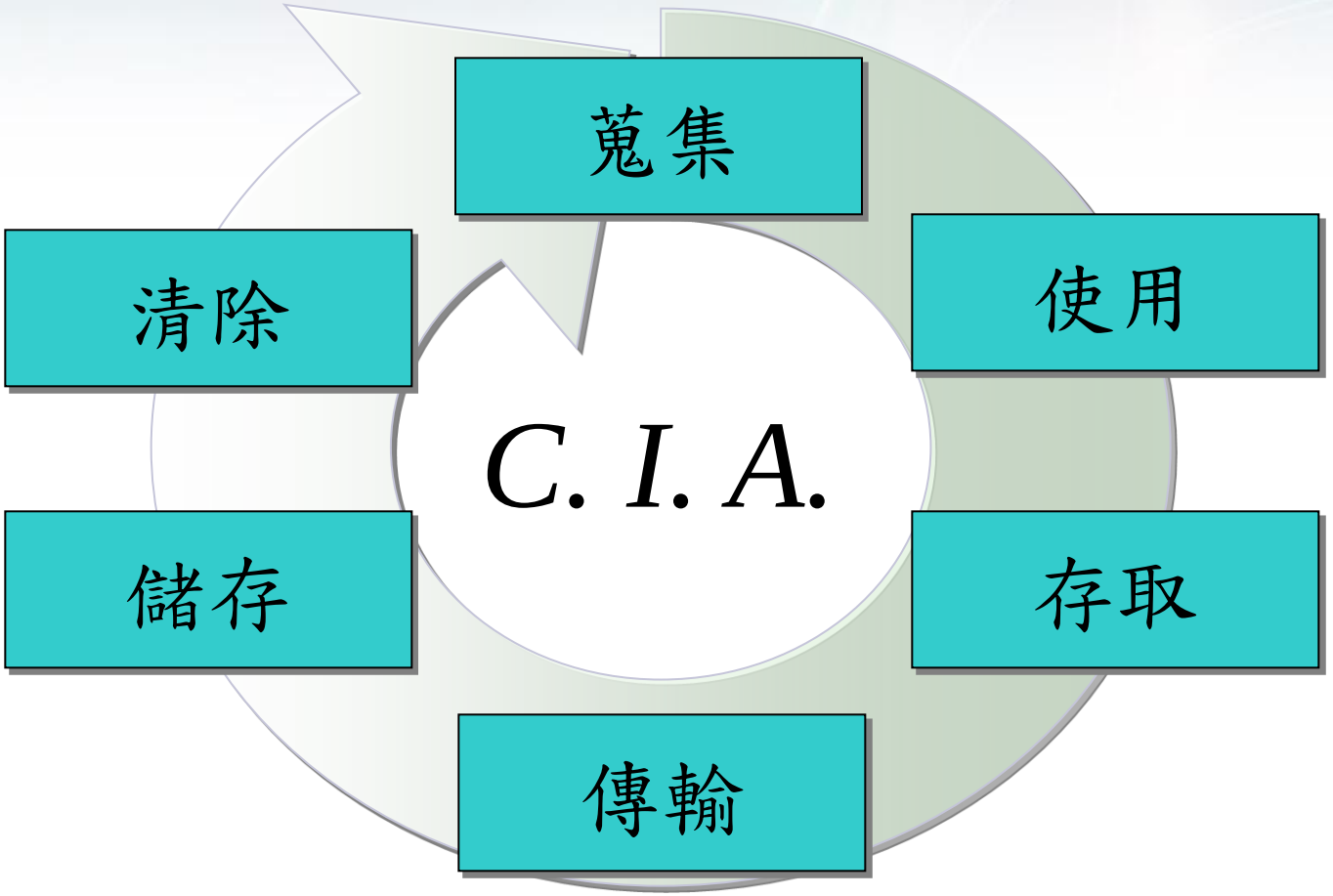
電腦處理個人資料保護法修訂草案(續)

- 實際影響
  - 將買賣個人資料行為從告訴乃論罪修改為公訴罪，並提高刑責，最高為五年有期徒刑
  - 寄廣告信、垃圾郵件將觸法，未經個人同意，網路公司或個體戶大舉販賣蒐集的大筆電子郵件信箱供寄發垃圾郵件等行為，均將觸犯本法，檢警接獲檢舉後必須主動追查
  - 若是公務員涉案，依法得加重其刑二分之一，最重可處七年半徒刑，與刑責已接近涉及貪瀆案
  - 重罰意圖營利而違法的行為，修訂草案大幅加重「意圖營利而違法蒐集、利用或盜賣個人資料者」的刑責，由原本二年以下徒刑，提高為五年以下徒刑，且併科由原先四萬元大幅提高為五百萬元罰金

個資案例

- **聯合報 *2008-08-27***
  - **竊5千萬筆個資 馬扁「搜」得到**
  - 國安大漏洞！刑事局昨天破獲兩岸駭客聯手入侵政府機關網站盜取個人資料、販賣牟利，包括現任總統馬英九、卸任總統陳水扁和王卓鈞、侯友宜等國安情治首長的個人資料，只要花*300*元，全都一覽無遺。警方說，查獲的資料庫多達*5,000*多萬筆，而且「只要想到的人都有」，相當驚人！
  - 陳光著集團**至少從健保局、教育部、戶政、各家電信公司、東森購物等多處管道入侵盜取個資**，同一人的個資被重複盜取，因此累計達五千萬筆，超出台灣*2,300*萬人口數一倍多，是歷年破獲最大宗盜取個資集團，依妨害電腦使用罪、詐欺、洗錢等罪嫌送辦
  - 偵九隊說，入侵駭客來自大陸，以中、北部大學網站當跳板入侵政府機關

個人資料生命週期管理
(Personal Data Life Management)



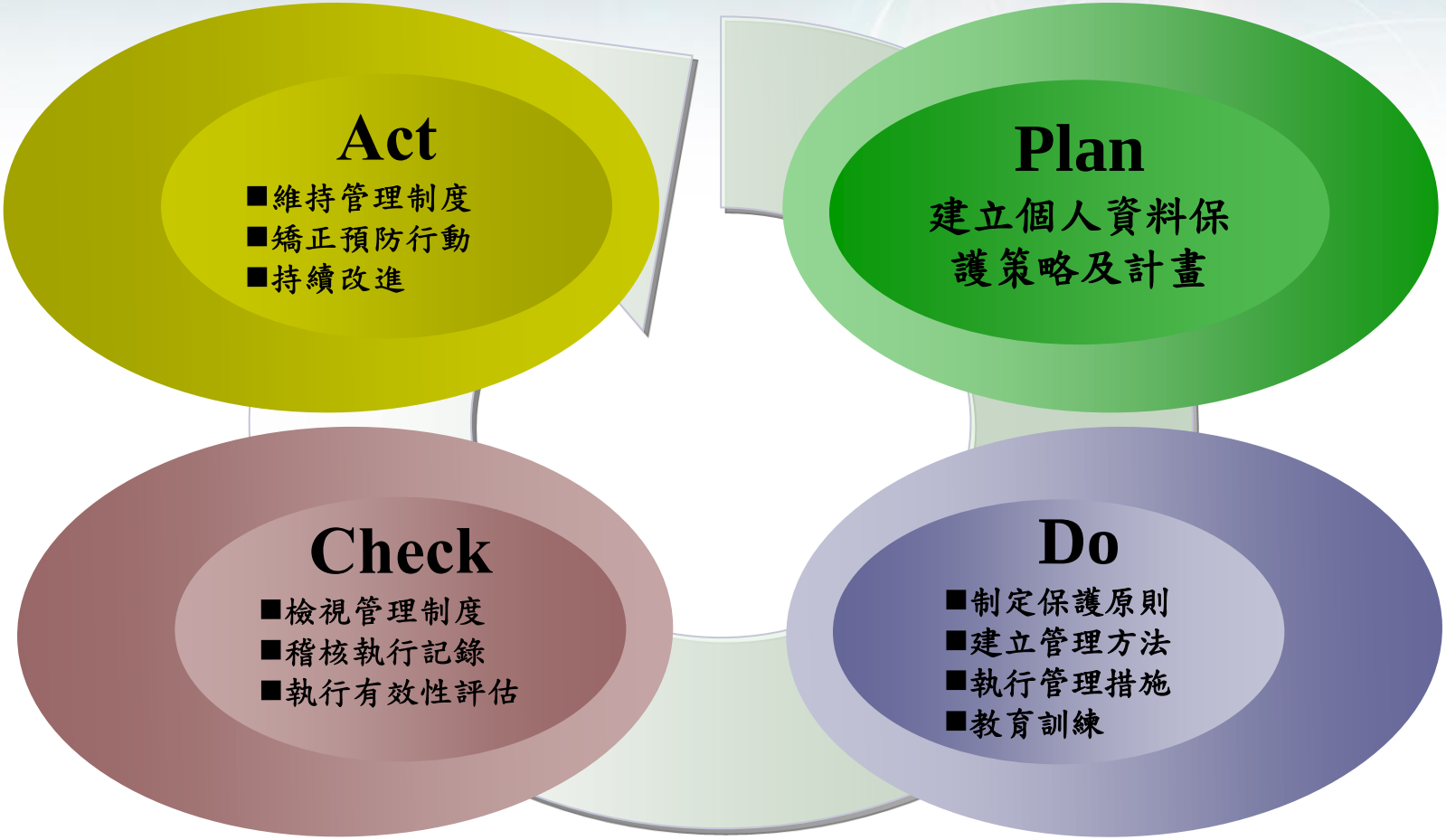
個人資料管理重點(一)

- 蒐集
  - ✓蒐集個人資料之理由、方法與告知義務
  - ✓確認個人資料之正確性及內容是否為法律定義之「得以直接或間接方式識別該個人之資料」
- 使用
  - ✓符合法律之使用規範
  - ✓符合組織政策之內部使用規範(例如：交叉行銷)
- 存取
  - ✓存取個人資料之權限管理
  - ✓委外或外包廠商之資訊安全管理

個人資料管理重點(二)

- 傳輸
  - ✓個人資料傳輸過程中之安全(加密或安全網路)
- 儲存
  - ✓個人資料新增及修改之作業程序
  - ✓存放個人資料場所及設備之安全管理
  - ✓備份或歸檔後之資料安全
- 清除
  - ✓個人資料刪除或報廢之安全處理程序
- 其它
  - ✓客訴、法律糾紛、懲處程序

個人資料保護之PDCA架構



個人資料保護管理措施
(以JISQ15001:2006為例)

Plan

1.將政策及目標文件化
2.建立專責組織
3.建立執行計畫

Do

1.對組織全員進行宣導
2.確認個人資料涵蓋範圍
3.辨識相關法令及規定
4.鑑別風險並管理風險
5.確認必要資源
6.制定相關規範
7.實施教育訓練
8.落實執行相關控管措施

Check & Act

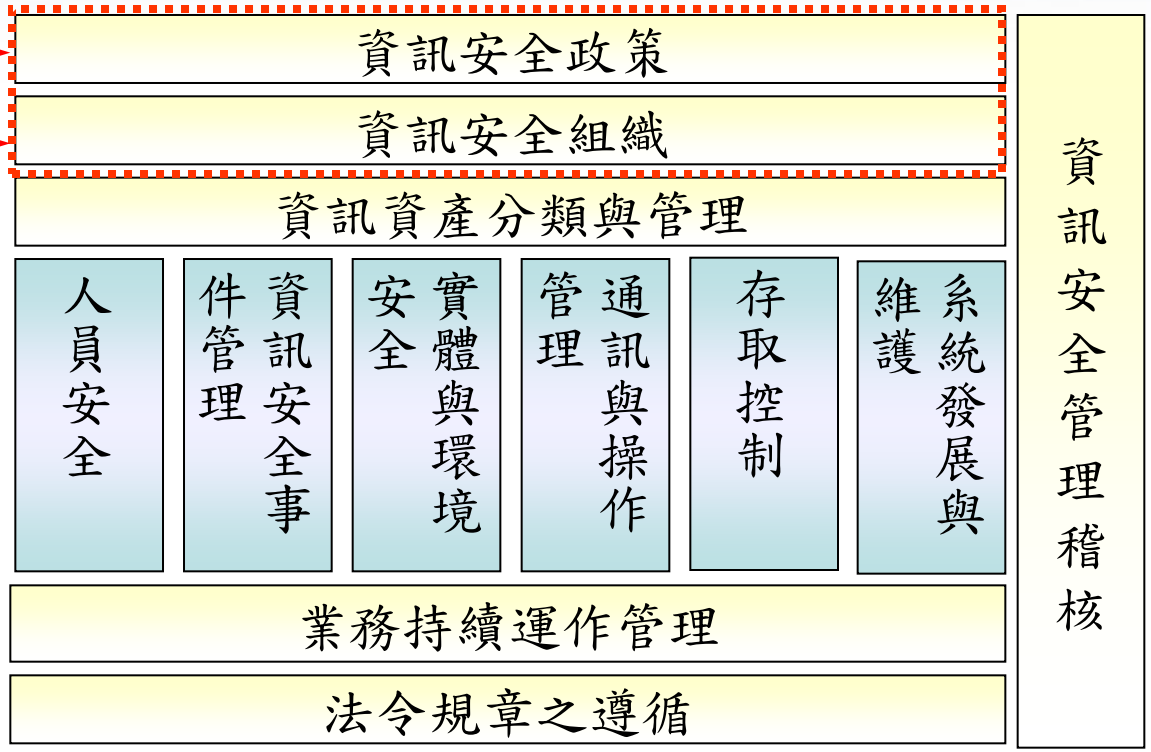
1.監督檢視管理成效
2.執行矯正預防措施

JISQ vs. ISO27001

JISQ 15001の Plan

1. 將政策及目標文件化
2. 建立專責組織
3. 建立執行計畫

ISO 27001 資訊安全管理內容



JISQ vs. ISO27001

JISQ 15001の Do

1.對組織全員進行宣導

2.確認個人資料涵蓋範圍

3.辨識相關法令及規定

4.鑑別風險並管理風險

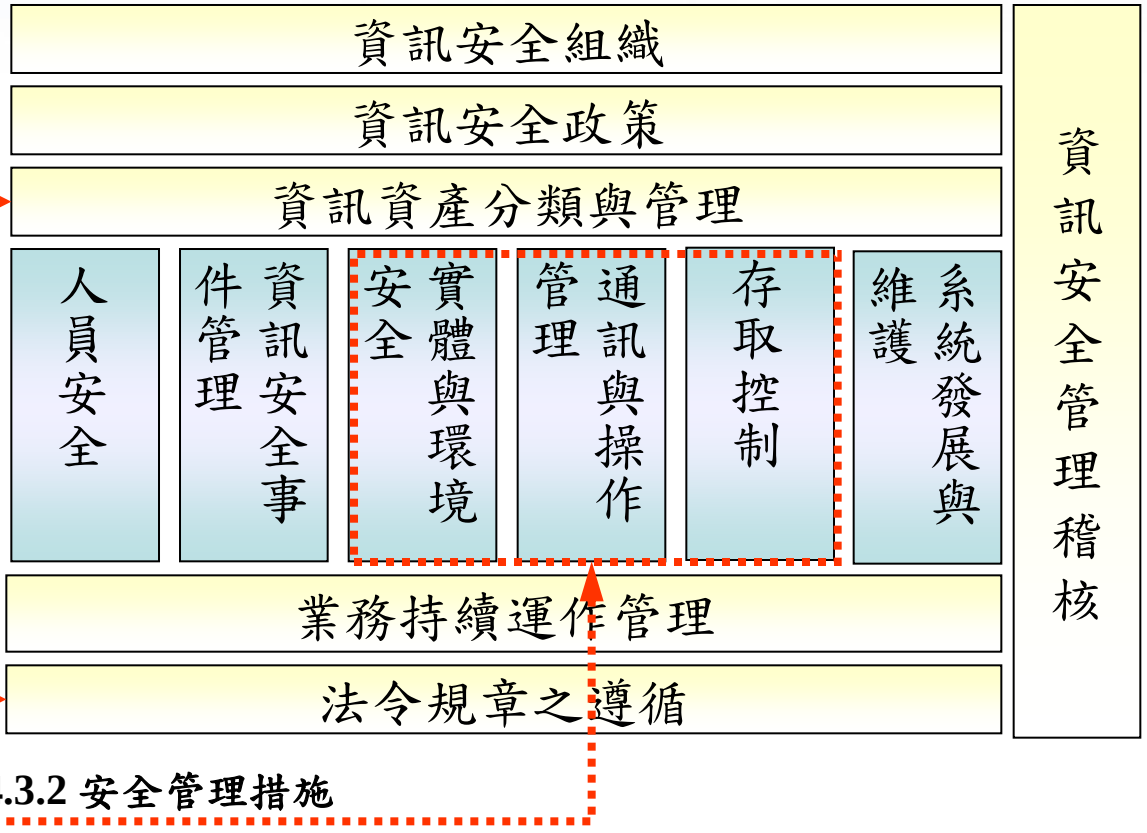
5.確認必要資源

6.制定相關規範

7.實施教育訓練

8.落實執行相關控管措施

ISO 27001 資訊安全管理內容



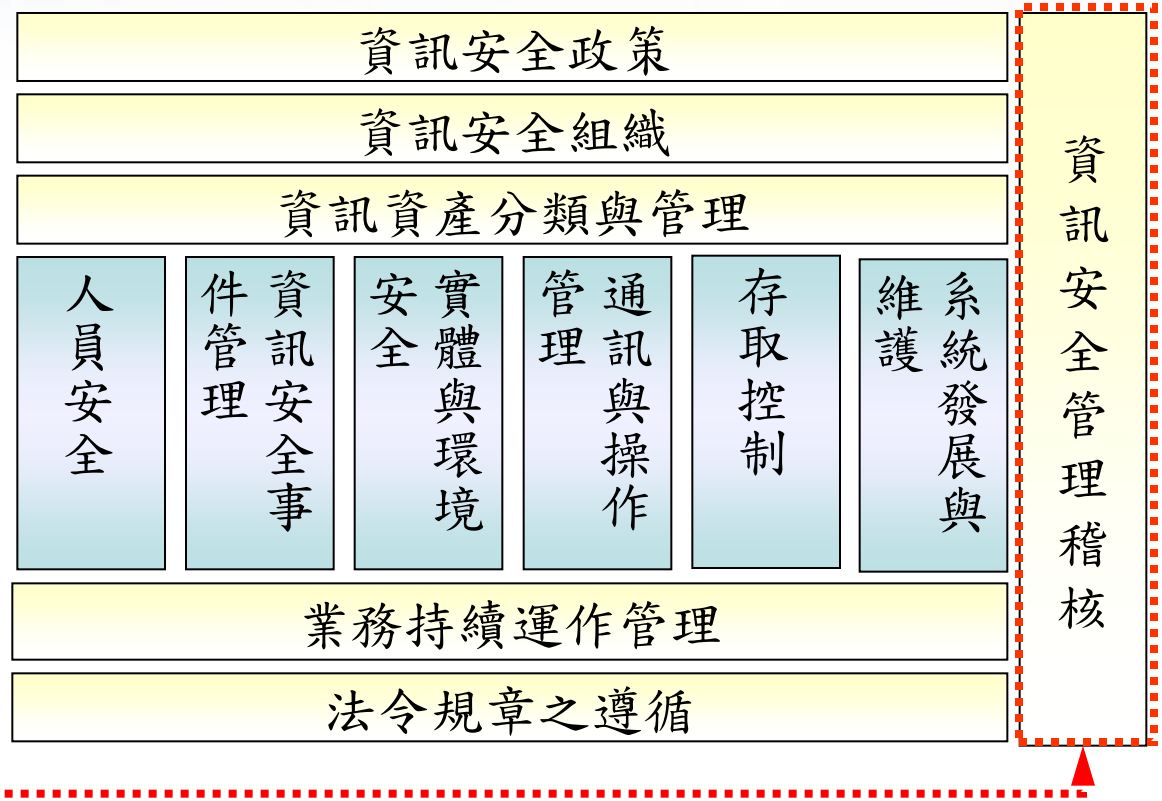
JISQ vs. ISO27001

JISQ 15001の

Check & Act

1. 監督檢視管理成效
2. 執行矯正預防措施

ISO 27001 資訊安全管理內容



保護個人資料小提醒

- ◆員工資料亦受法律保護
- ◆所有調閱活動應依照標準作業程序進行
- ◆不在電話裡隨便透露個人資料
- ◆非信任之網站，勿隨意留下個人資料
- ◆以碎紙機銷毀各式帳單、收據、信件、藥單等
- ◆不點選不明人士傳送的網址
- ◆提防偽裝之網頁、電子報與信件
- ◆不委託他人代辦貸款及信用卡
- ◆影印文件交付時註明用途(表示不適用於其他用途)

簡報完畢，敬請指教