面對資安法：
如何做好第一道防線？
認識法規與制度

撰寫人

EY 安永
Building a better working world

安永企業管理諮詢服務股份有限公司

曾品媛
資深經理， 企業管理諮詢服務
聯絡電話：+886 2 2757 8888 ext.67814
電子郵件： Jenny.Tsen@tw.ey.com

背景介紹

- ▶ 安永企業管理諮詢服務股份有限公司經理。
- ▶ 專長於資訊安全、電腦稽核、營運持續管理及個人資料保護管理系統。
- ▶ 曾從事電腦稽核、風險管理、資訊安全管理制度及個人資料管理制度導入等相關服務。

相關經驗介紹

- ▶ 擔任專案經理協助數個政府單位導入ISO 27001:2013並順利取得證書。
- ▶ 擔任專案經理協助某金融機構同時導入ISO 27001:2013 及BS10012:2009 管理制度。
- ▶ 曾協助某傳統產業評估其內控管理制度與SOX間之差異並提出改善建議。
- ▶ 擔任專案經理協助國內知名之保全業導入ISO 27001:2013 並取得證書。
- ▶ 擔任專案經理協助某外商保險公司評估其海外災害復原機制是否有符合法規要求。
- ▶ 擔任專案經理協助某IC公司執行ISO27001:2013差異分析及風險評鑑作業。
- ▶ 曾協助某外商銀行執行其供應商之資訊安全環境評估並提出改善建議。
- ▶ 曾協助某市政府資訊單位執行 資訊安全管理系統導入並順利通過 ISO 27001:2005 認證。
- ▶ 曾輔導數家大專院校執行資訊安全管理系統導入並順利取得 ISO 27001:2005 認證。
- ▶ 曾協助某政府單位執行資訊系統稽核專案，檢視內部控制制度資訊循環項目，根據相關辦法進行查核並給予建議。

學歷及專業資格

- ▶ ISO 27001:2013 LA
- ▶BS 25999 LA
- ▶國際專案管理師 PMP
- ▶國際資訊安全經理人 CISM
- ▶臺灣大學 GMBA 碩士學位
- ▶美國阿拉巴馬州立大學學士主修 Computer Science

大綱

大綱

網路安全知多少? (1/3)

以下哪個選項是當今組織面臨最大的安全威脅之一?

A. 社交工程
B. 網路駭客
C. 網站竄改
D. 資金遭竊盜

網路安全知多少? (1/3)

以下哪個選項是當今組織面臨最大的安全威脅之一?

A. 社交工程

B. 網路駭客

C. 網站竄改

D. 資金遭竊盜

Social Engineer Inc 顯示，90%的人在提供電子郵件地址時並不會確認對方的身份，高達67%的人會提供身份證字號，出生年月日或員工編號。

網路安全知多少? (2/3)

員工離職或遭雇主解僱時，偷取組織重要資訊的百分比是多少？

A. 低於 5%

B. 10 到 20%

C. 30 到 40%

D. 超過 50%

網路安全知多少? (2/3)

員工離職或遭雇主解僱時，員工偷取組織重要資訊的百分比是多少？

A. 低於 5%

B. 10 到 20%

C. 30 到 40%

D. 超過 50%

網路安全知多少? (2/3)

員工離職或遭雇主解僱時，員工偷取組織重要資訊的百分比是多少？

A. 低於 5%

B. 10 到 20%

C. 30 到 40%

D. 超過 50%

根據Ponemon研究所的數據，59%的員工在離開雇主時竊取了組織重要資訊。

網路安全知多少? (3/3)

當發生入侵事件到該事件被發現平均時間為何?

A. 超過六個月
B. 約三個月
C. 約一個月
D. 約一週

網路安全知多少? (3/3)

當發生入侵事件到該事件被發現平均時間為何?

A. 超過六個月

B. 約三個月

C. 約一個月

D. 約一週

根據“MandiantM趨勢”2015年報告，攻擊者潛伏在組織內等待攻擊的天數平均為205天; 69%的組織是從外部單位得知相關漏洞（如執法機構）。

資安事件分享


時間軸
109 04/06
[科技業]系統漏洞
Zoom官方證實將資料「誤傳」給中國！多國政府單位、知名企業都宣布禁用
109 04/09
[科技業]勒索病毒
群創網路中毒？被勒索病毒攻擊但生產未受影響
109 04/19
[科技業]個資外洩
逾50萬Zoom帳號 遭暗網賤賣
109 04/20
[演藝]個資外洩
韓星河正宇個資外洩遭勒索15億！
109 05/04
[石化工業]勒索病毒
中油資料庫和部分電腦主機遭勒索軟體感染，斷網防受駭範圍擴大，暫通報為三級資安事件
109 05/05
[政府機關]個資外洩
日本愛知縣武漢肺炎確診者個資外洩，共495人

資安事件分享

時間軸

109 05/05 [石化工業]惡意程式攻擊

- 加油站連爆資安事件！繼中油後，台塑化系統也遭駭客攻擊

109 05/08 [金融業]人員疏失

- 洛杉磯分行遭詐！台銀：非資安漏洞 坦承人員處理疏失

109 05/10

- 天才駭客？ 美15歲少年遭控竊取價值7.23億加密貨幣

109 05/12

- 駭客論壇驚見兜售67萬筆知名餐飲3年前外洩顧客帳密，饗食天堂雖早已翻新網站，但仍緊急通知顧客換密碼。

109 05/05 [科技業]勒索病毒

- 獨家》力成也遭勒索病毒攻擊 疑不只3家企業遇駭

109 05/10 [政府機關]個資外洩

- 77萬移民資料全外洩？澳洲內政部爆漏洞 申請資料被看光…

109 05/11 [學校]木馬程式

- 【台體大暴君4】情蒐室被植木馬不理 職棒機密全外洩。

EY安永

資安事件對組織的影響

教育學程報名系統疑個資外洩 台大：已修復補強

2021/6/3 18:45

（中央社記者許秩維台北3日電）前台大學生會長吳奕柔今天在臉書發文，質疑台大師培中心教育學程報名系統個資外洩；台大校方表示，已修復補強系統並重新上線，學校將檢討並強化資安和個資保護。

台灣大學前學生會長吳奕柔在臉書發文指出，昨天晚上登入台大師資培育中心的教育

台大成績系統遭駭 人人87分！背後竟是資工系學生 | 生活 | 三立新 ...
https://www.setn.com/News.aspx?NewsID=632065

2019/11/8 · 台灣大學6日傳出ceiba成績登分系統遭駭客入侵，學生成績清一色被竄改成87分，引起熱烈討論。台大校方今（8）發出聲明澄清，系統並不是駭客入侵 ...

預估閱讀時間: 9 分鐘

台大平台成績全被改87分 原是資工系學生抓漏洞 - 生活 - 自由時報 ...
https://news.ltn.com.tw/news/life/breakingnews/2971370

2019/11/8 · 台灣大學教務處的數位教學平台（CEIBA）6日被人發現，學生全部的平時成績都被改成87分，經查是校內資工系學生進行資訊安全漏洞研究，不小心 ...

預估閱讀時間: 3 分鐘

台大成績遭駭87分！竟是資工系學生 | 三立新聞網 | LINE TODAY
https://today.line.me/tw/v2/article/G65Yq8

台灣大學6日傳出ceiba成績登分系統遭駭客入侵，學生成績清一色被竄改成87分，引起熱烈討論。台大校方今（8）發出聲明澄清，系統並不是駭客入侵，而是學校資工系的學生在做研究時不小心修改造成的烏龍事件。 台大成績系統傳出遭駭，學生分數被 ...

預估閱讀時間: 2 分鐘

- 違反法令法規
- 組織聲譽受損
- 失去市場及客戶信心
- 業務中斷
- 直接或間接財務影響
- 競爭優勢受到危害
- 企業終止營運

2021 年網路安全趨勢預測

1 以疫苗為誘餌的網路釣魚活動

由於新冠肺炎疫情仍未停歇，網路釣魚活動將繼續利用疫苗開發或各國新增限制措施的消息；有意竊取疫苗資訊的網路犯罪分子或國家也將持續鎖定開發疫苗的製藥公司作為攻擊目標。

2 鎖定遠距辦公的攻擊未歇

駭客擴大對遠距辦公人員的「執行緒劫持」（Thread Hijacking）攻擊，利用 Emotet 和 Qbot 木馬竊取資料或潛入網路，影響全球 24% 企業。此外，針對遠端桌面協定（RDP）和 VPN 等遠端存取系統的攻擊也急劇增加。目前全球的中小學及大專院校大幅採用電子教學平台，在新學期開始前的八月，教育業每週遭遇的網路攻擊數量增加 30%。未來一年，可預期網路攻擊將繼續干擾遠距學習的進行。

3 雙重勒索攻擊數量急據上升

在 2020 年第三季，近半的勒索軟體攻擊事件威脅企業將曝光內部資料；數據顯示，全球平均每 10 秒就有一個新企業遭受勒索軟體攻擊，其中，醫院是最容易遭到雙重勒索攻擊且最具吸引力的目標之一。

資料來源：https://www.inside.com.tw/article/22034-CheckPoint-cyber-security-2021

2021 年網路安全趨勢預測

4 深度偽造技術（Deep fakes）成為武器

現今偽造影片或音訊的技術現在已相當先進，能用於創造特定內容，成為操縱輿論、股價或更惡劣的目的的武器，更簡單的深度偽造應用可能偽造音訊發起語音網路釣魚，例如透過偽造公司執行長聲音通過語音身份驗證。今年初，比利時某政治團體發佈了一則關於比利時總理的深度偽造影片，總理在影片中將新冠肺炎歸因於環境破壞，並呼籲採取行動來應對氣候變化，許多觀眾都信以為真。

5 優勢與挑戰並存的 5G 網路

打造一個萬物互聯的高速世界，卻也導致犯罪分子和駭客擁有了更多攻擊機會，如電子醫療裝置監測使用者的健康狀況，聯網汽車服務掌握使用者的移動路徑，智慧城市應用則會記錄下使用者的生活方式。為了保護個人隱私，我們需要更全面地保護 5G 裝置中的大量資料，防止資料遭洩露、盜竊和篡改，尤其須注意許多資料可能繞過公司網路及其安全控制。

資料來源：https://www.inside.com.tw/article/22034-CheckPoint-cyber-security-2021

網路釣魚手法

釣魚郵件詐騙

一個假的電子郵件，看似來自受害者知道的人或公司，通常包含至少一個附件或連結。附件通常會夾帶病毒，而連結會進入被設計成仿似合法公司的假網站，誘使收件者提供資料。

假的搜索 真的詐騙

透過付費的廣告讓他們顯示在搜索結果頁面的頂部。這些搜索結果看似真的，用以引誘那些想要修復電腦的受害者。但當您點擊該廣告，病毒就會開始下載到您的電腦，盜取您的個資讓電腦產生問題。

語音詐騙

彈出式警告詐騙

在瀏覽網站時，以小圖或廣告時出現在螢幕上。彈出訊息通常會與瀏覽過的內容相關，並連接到其他網站，出現類似內容或商品。

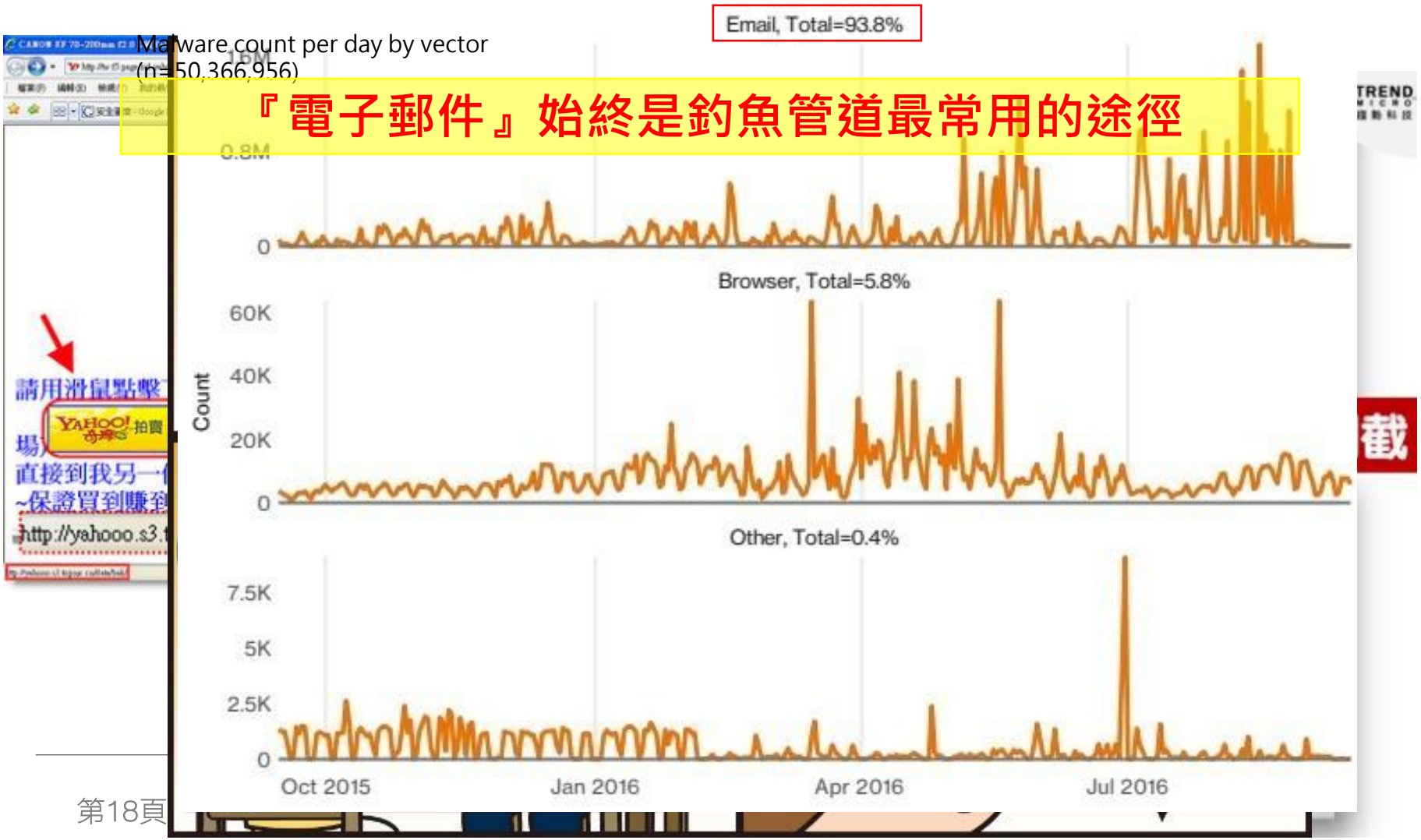
技術支援詐騙

詐騙者宣稱來自資安公司並撥打給受害者。他們以話術欺騙受害者，告知在受害者的電腦上發現病毒。詐騙者假裝可以提供解決方案，在用戶的電腦裡安裝某種遠程桌面監控軟體、惡意軟體或要求支付費用”修復”電腦問題。

資料來源：
https://www.jadespring.com.tw/%E5%A6%82%E4%BD%95%E9%98%B2%E8%AD%B7%E4%BA%94%E7%A8%AE%E5%B8%B8%E8%A6%8B%E7%9A%84%E7%B6%B2%E8%B7%AF%E9%87%A3%E9%AD%9A%E8%A9%90%E9%A8%99.html

網路釣魚攻擊不再侷限於電子郵件

常見釣魚的管道



網路釣魚攻擊不再侷限於電子郵件(續)

Deep Fake深偽技術

BuzzFeed與演員Jordan Peele 4月時在YouTube發布、以FakeApp製成的「深度造假」影片

網路釣魚攻擊不再侷限於電子郵件(續)

- Deep Fake深偽技術
  - AI語音模仿老闆聲音要求轉帳，成功騙走近770萬元

行動惡意軟體攻擊加劇

- 與2018年相比，2019上半年銀行惡意軟體攻擊增加50%。
- 攻擊也越趨複雜，可誘使行動裝置使用者點擊惡意網站連結。
  - 藉由改良技術來繞過安全防護措施，將惡意應用程式植入官方App商店中。
  - 利用大型國際公司的行動裝置管理系統（MDM）將惡意軟體發送到超過75%所管理的行動裝置
- 未來駭客願意付錢就能買到新版本行動惡意程式。

行動惡意軟體攻擊加劇(續)

- 惡意程式植入Store

www.ithome.com.tw › news

蘋果App Store有17款程式含木馬元件| iThome

2019年10月25日 - 這些被植入「點擊木馬模組」的iOS程式，全來自AppAspect Technologies，會在裝置背景執行廣告詐騙活動，還可連結駭客所掌控的C&C伺服器 ...

3c.ltn.com.tw › news

Android用戶注意！11款App藏有惡意程式竊個資、還會偷扣款 ...

2020年7月12日 - ... 商店發現共有11款遭Joker惡意間諜軟體植入的應用程式，透過假借為 ... 等工具類型的App名稱上架到Play Store 平台上，除了會隱身於程式碼 ...

3c.ltn.com.tw › news

你也中招了嗎？85款假冒相機與遊戲Android App 遭惡意廣告入侵

2019年8月17日 - Google Play Store 多達85款的Android App免費應用程式，被資安業者 ... 遭植入惡意廣告活動的App，當用戶在安裝到Android手機後，會自動於 ...

www.taiwannews.com.tw › news

惡意軟體入侵蘋果App Store 微信也中招| 台灣英文新聞

2015年9月21日 - 中央社紐約20日綜合外電報導）蘋果公司旗下iOS App Store首度遭到大規模攻擊，開發商誤用植入惡意軟體的Xcode寫程式，因此寫出許多有毒 ...

大綱

資訊安全相關法令

資通安全管理法
資通安全管理法6子法

個人資料保護法
個人資料保護施行細則

國家機密保護法
國家機密保護法施行細則

著作權法

刑法第 36 章妨害電腦使用罪

刑法第 36 章妨害電腦使用罪

第 358 條
無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 359 條
無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 360 條
無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 361 條
對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
第 362 條
製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

其他相關法令

- 除了違反智慧財產權、侵害隱私權、電腦犯罪，其他常見的網路犯罪類型尚有：
  - 妨害風化
  - 網路竊盜
  - 網路詐欺
  - 偽造文書
  - 煽惑他人犯罪

其他相關法令--妨害風化

- **網路援交**
  - 刊登網路援助交際訊息
  - 違反兒童及少年性交易防制條例第29條之「以電腦網路散布使人為性交易訊息罪」，最重可處有期徒刑五年

- **貼圖、以電子郵件散布色情圖片**
  - 圖片若為未滿十八歲之人：兒童及少年性交易防制條例第28條之「散布未滿十八歲之人性交或猥褻圖片罪」，最重可處有期徒刑三年
  - 圖片若已滿十八歲之人：刑法第235條散布猥褻圖片罪，最重可處有期徒刑二年

- **販賣色情光碟**
  - 同樣刑法第235條

其他相關法令--竊盜及詐欺

- **線上遊戲寶物、天幣竊盜**
  - 以竊盜罪移送。刑法第359條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者」最重可處有期徒刑五年
- **網路拍賣交易詐欺**
  - 刑法第339條，最重可處有期徒刑五年
- **不正當利用電腦取財**
  - 以不正當方法製作財產之變更，而取得他人財產者，刑法第339條之三第一項，最重可處有期徒刑七年

其他相關法令--偽造文書及煽惑犯罪

- **線上遊戲寶物、天幣竊盜**
  - 以竊盜罪移送。刑法第359條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者」最重可處有期徒刑五年
- **網路拍賣交易詐欺**
  - 刑法第339條，最重可處有期徒刑五年
- **不正當利用電腦取財**
  - 以不正當方法製作財產之變更，而取得他人財產者，刑法第339條之三第一項，最重可處有期徒刑七年

資通安全法

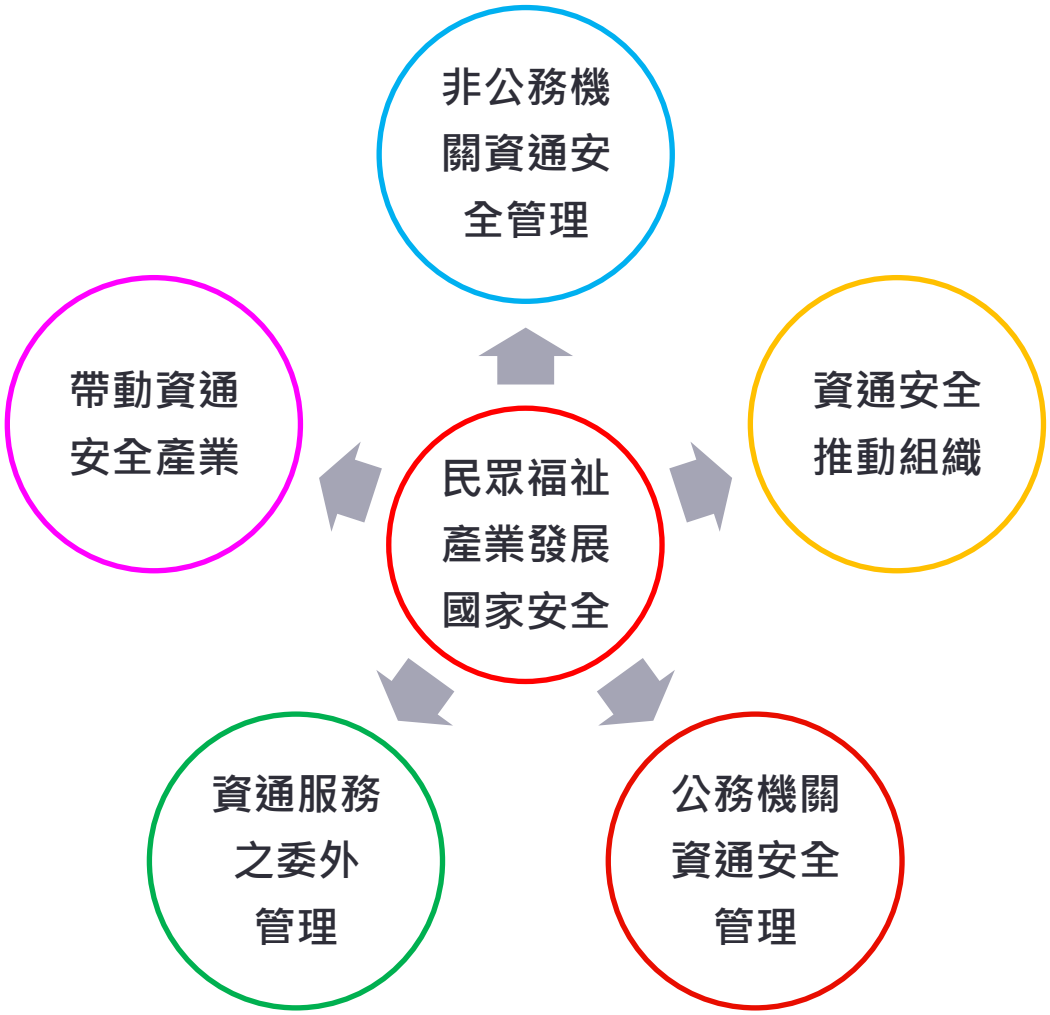
資安即國安

建立堅韌、安全、可信賴的智慧國家

制定資通安全管理法之目的

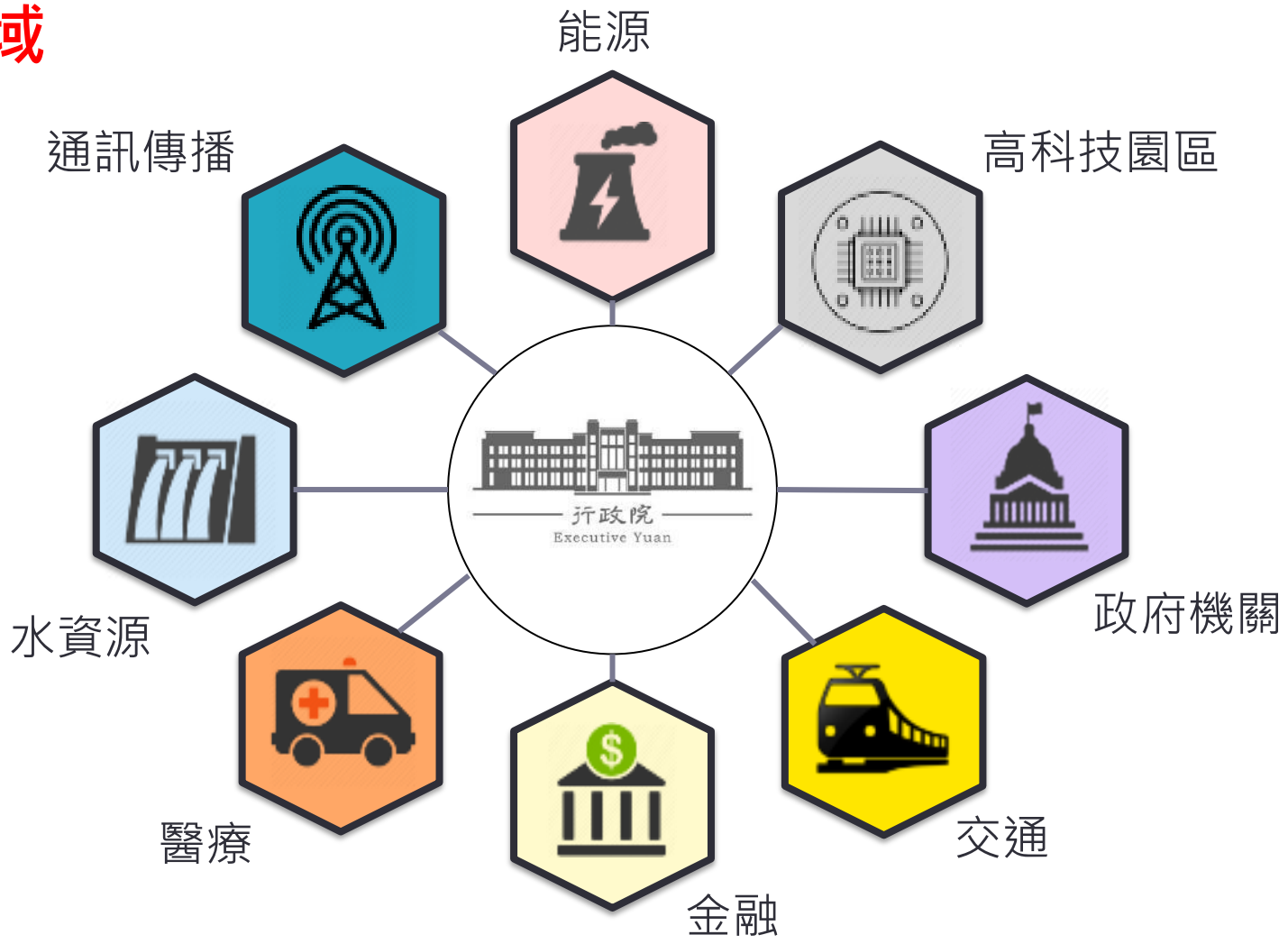
2019 年正式上路

- 網際網路發展及ICT應用的普及。
- Cyber Security & Critical Infrastructure (CI) Threats。
- 為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。

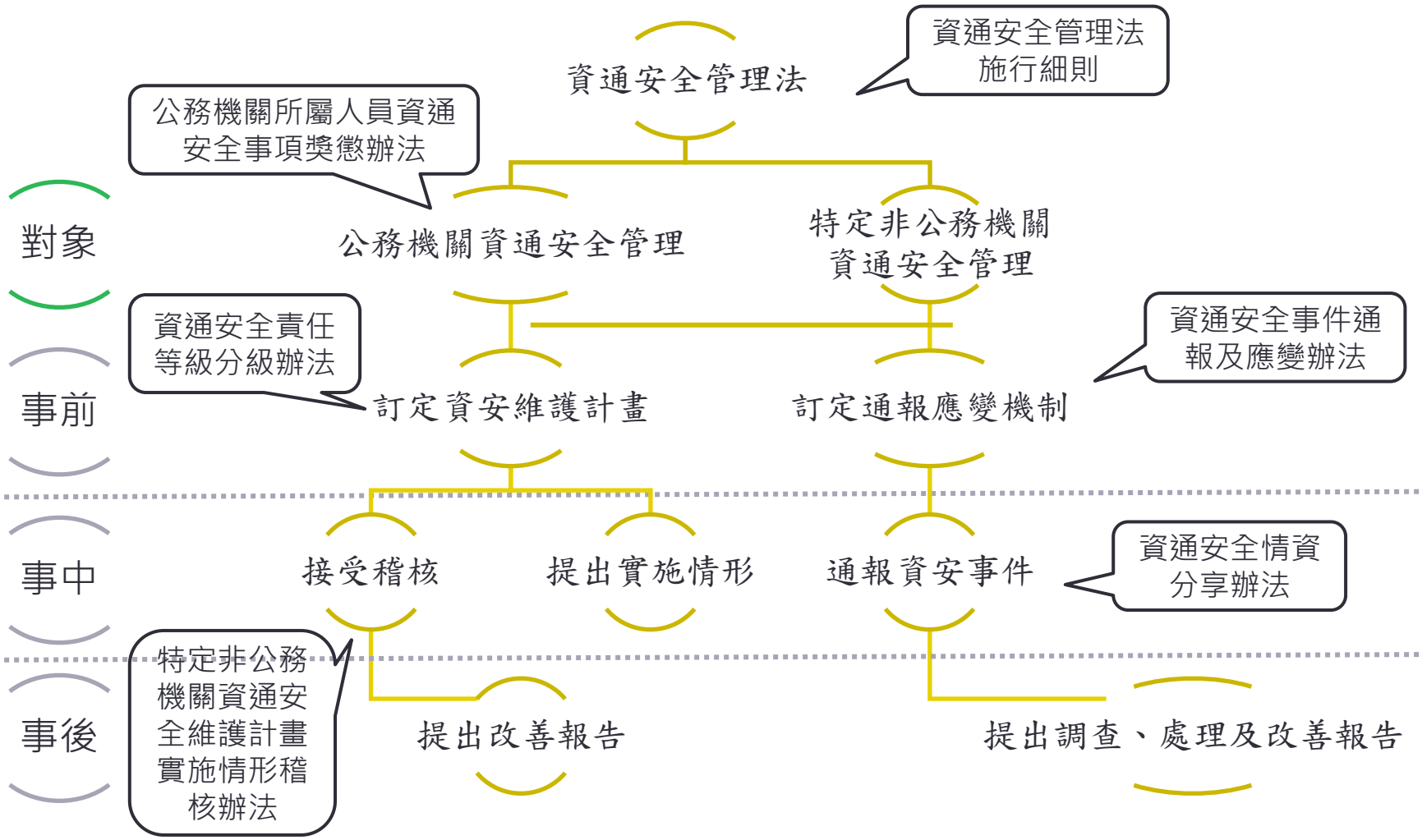


適用資通安全法的對象

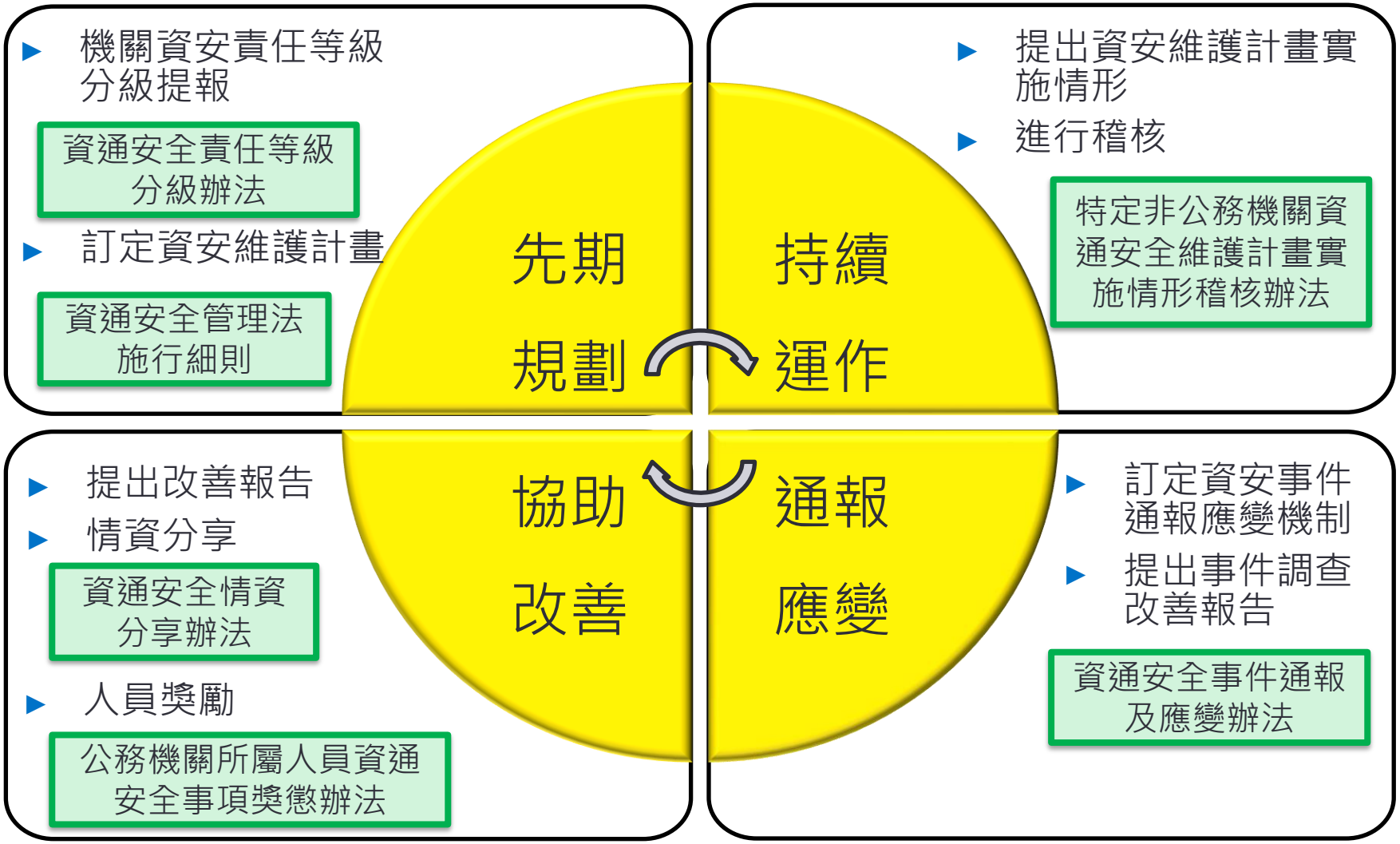
八大領域



資通安全及子法架構 1/2



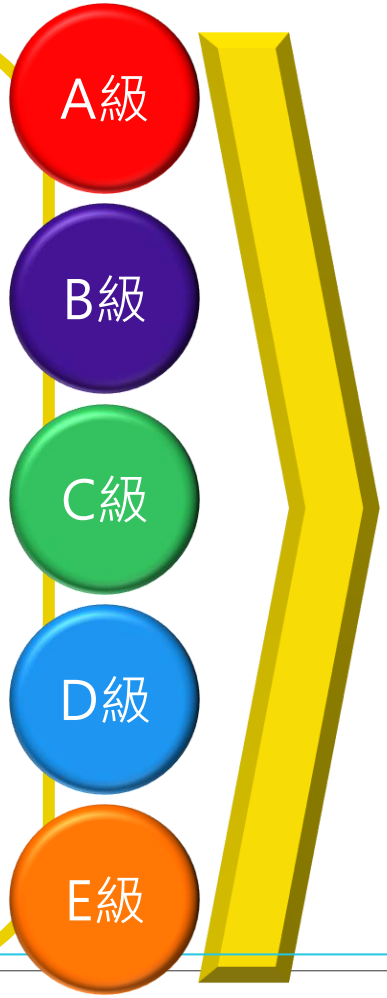
資通安全及子法架構 2/2



資通安全管理法的重要規範與實施近況

- 資通安全責任等級分級辦法1/5-分級

- 國家機密、涉及外交、國防、國土安全事項。
- 持有民眾或公務員個人資料檔案。
- 公務機關涉及能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項。
- 關鍵基礎設施服務，對社會公共利益、民心士氣，或民眾生命、身體、財產之影響。
- 資通系統服務民眾之範圍
- 跨公務機關共用性資通系統之服務範圍
- 醫院分級



機關應辦事項

- 管理面
- 技術面
- 認知與訓練

資通安全管理法的重要規範與實施近況

- **資通安全責任等級分級辦法 2/5-分級 (B極為例)**

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置二人；須以專職人員配置之。
	內部資通安全稽核		每年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
	資安治理成熟度評估		每年辦理一次。

資通安全管理法的重要規範與實施近況

- **資通安全責任等級分級辦法 3/5-分級 (B極為例)**

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。

資通安全管理法的重要規範與實施近況

- **資通安全責任等級分級辦法 4/5-分級 (B極為例)**

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	政府組態基準		初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。
	資通防護	防毒軟體	全部核心資通系統每年辦理一次。
		網路防火牆	全部核心資通系統每二年辦理一次。
		具有郵件伺服器者，應備電子郵件過濾機制	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	

資通安全管理法的重要規範與實施近況

- **資通安全責任等級分級辦法 5/5-分級 (B極為例)**

制度面向	辦理項目	辦理項目細項	辦理內容
認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年至少二名人員各接受十二小時以上 之資通安全專業課程訓練或資通安全職 能訓練。
		一般使用者及主管	每人每年接受三小時以上之一般資通安 全教育訓練。
	資通安全專業證照及職能訓練證書	網路防火牆 資通安全專業證照	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有二張以上，並持續維持證照之有效性。
		資通安全職能評量證書	初次受核定或等級變更後之一年內資通安全專職人員總計應持有二張以上，並持續維持證書之有效性。

個資法

新版個資法於2012年10月1日施行

個人資料保護法概說

電腦處理個人資料保護法 → 個人資料保護法

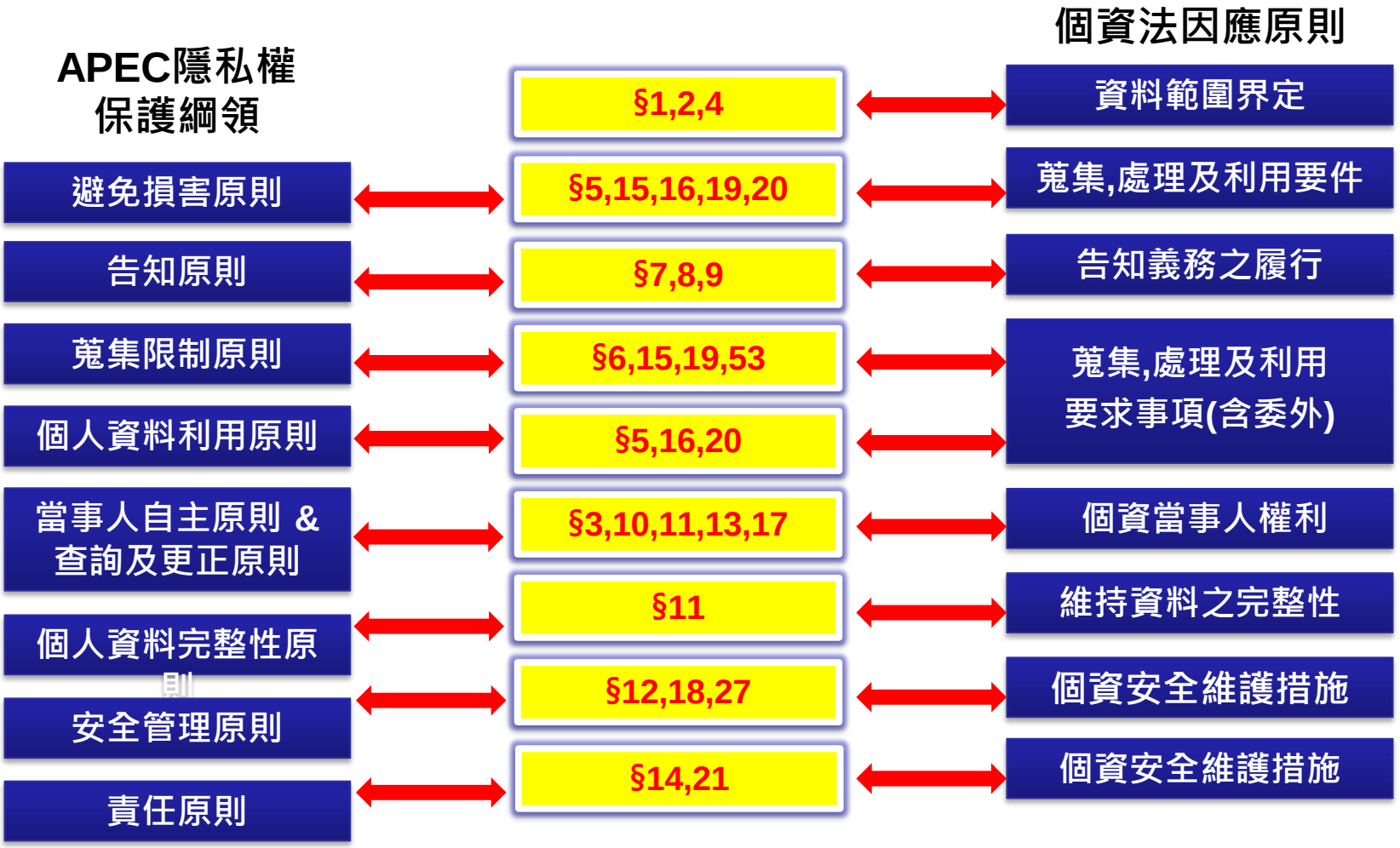
新法正式施行日101.10.01

OECD 個人資料保護八大原則	APEC 隱私權保護綱領
1.限制蒐集原則	1.預防損害原則
2.資訊內容完整正確原則	2.告知原則
3.目的明確化原則	3.蒐集限制原則
4.限制利用原則	4.個人資料利用原則
5.安全保護原則	5.當事人自主原則
6.公開原則	6.個人資料完整性原則
7.個人參加原則	7.安全管理原則
8.責任原則	8.查閱及更正
	9.責任原則

OECD 資料保護八原則

- 原則一：公平合法的處理；
- 原則二：僅限合於特定目的之取得，且不會進行不符合特定目的之後續處理；
- 原則三：適當、相關，且不過度；
- 原則四：正確且最新；
- 原則五：保存期間不超過必要期限；
- 原則六：依據法律授予個人權利進行處理，包含行使調閱權；
- 原則七：確保安全；
- 原則八：不會在無適當防護下，被移轉到對個人資訊未有適當保護要求之地區；

個人資料保護法與APEC隱私權保護綱領



個人資料保護法的重點彙整

	新個人資料保護法
擴大適用範圍	全體企業均有適用
擴大保護客體	不以經電腦處理之個人資料為限 ，及於紙本個資 （**個資風險防範不再僅限於資訊安全**）
下放行政監督權至地方層級	除中央目的事業主管機關外**直轄市、縣市政府亦得進行檢查或命說明**
提高行政責任	行政責任部分最高可處新台幣（下同）5萬元以上50萬元以下罰鍰 **及公布「違章情形」、「企業名稱」及「負責人姓名」（商譽損失）**
植入雙罰規定	企業遭行政罰時，會同時處罰企業負責人（除非負責人能舉證已盡注意能事）

個人資料保護法的重點彙整(續)

	新個人資料保護法
提高刑事責任	意圖營利違法蒐集、處理、利用及違反主管機關禁止國際傳輸命令者，足生損害於他人者，處5年以下有期徒刑或併科100萬元以下罰金 【意圖營利】屬於特別主觀構成要件，不以客觀上確有發生營利結果為刑罰要件，只要是為了增加營業收入或其他經濟利益而蒐集處理或利用個資（例如各種行銷行為），一旦違反新版個資法，仍有本條之風險。
提高民事責任	同一原因事實造成多數人損害，受害人最高可請求賠償額**達2億元**。但企業所涉利益超過2億元者，以企業所涉利益作為賠償上限之認定 不易/不能證明其實際損害額時，得請求法院依侵害情節，以每人每件500~20,000元計算

個人資料保護法的重點彙整(續)

	新個人資料保護法
舉證責任倒置	採取過失責任制度，但由企業負擔舉證證責任，舉證其已盡善良管理人之注意義務。
引入團體訴訟機制	20人以上即得以書面授權公益團體代行訴訟（須防範個資蟑螂）

公開發行公司建立內部控制制度處理準則修正

- 金管會於2014年9月3日發布修正「公開發行公司建立內部控制制度處理準則」條文。
- 強調公司治理觀念及配合國內實務需要，為規範公司妥善管理個人資料之蒐集、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，將個人資料保護管理等納入控制作業。

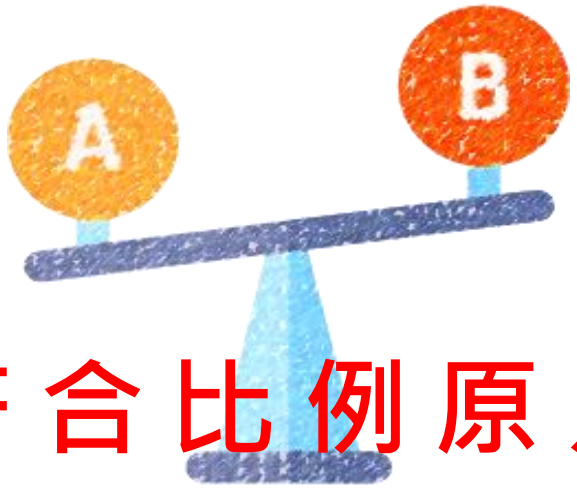
公司須制訂個人資料保護管理之內部控制作業程序，並經董事會同意通過。

個人資料保護法立法目的

■個資法 第1條 (保障人格權，促進個人資料之合理利用)

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。

保護



合理利用

符 合 比 例 原 則

個人資料保護法立法目的

■ 保障人格權，促進個人資料之合理利用。

個人資料保護法§1：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。

個人資料保護法立法目的(續)

■ 保障個人「資訊自主決定權」。

個人資料保護法§3：當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一、查詢或請求閱覽。
二、請求製給複製本。
三、請求補充或更正。
四、請求停止蒐集、處理或利用。
五、請求刪除。

案例分享

重機囂張假車牌　在大陸購物網站買的到

2015年06月10日

每日免費文章尚餘0篇 facebook

有名的大型重機假車牌「BS-81」在路上出現。(翻攝自【重機車友　|各區路況、天氣回報中心】)

資料來源：https://www.nextmag.com.tw/realtimenews/news/20896810

個人資料保護法立法目的(續)

■ 保障資訊隱私權。

個人資料保護法§18及§27(摘錄)：
為防止個人資料被竊取、竄改、毀損、滅失或洩漏，
一、 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項；
二、 非公務機關保有個人資料檔案者，應採行適當之安全措施。

個人資料定義

- 個人資料（§2）
  - ✓ 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、醫療、基因 、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
  - ✓ 間接方式（施細 §3）
    - 間接方式識別該個人之資料，指僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別該特定個人者。例如，員工編號、保單號碼。

不適用個人資料保護法之情形

■個資法 第51條

有下列情形之一者，不適用本法規定：

一、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。

例如，朋友間交換手機號碼。

取得朋友的聯絡電話、地址等資訊

不適用個人資料保護法之情形

■個資法 第51條

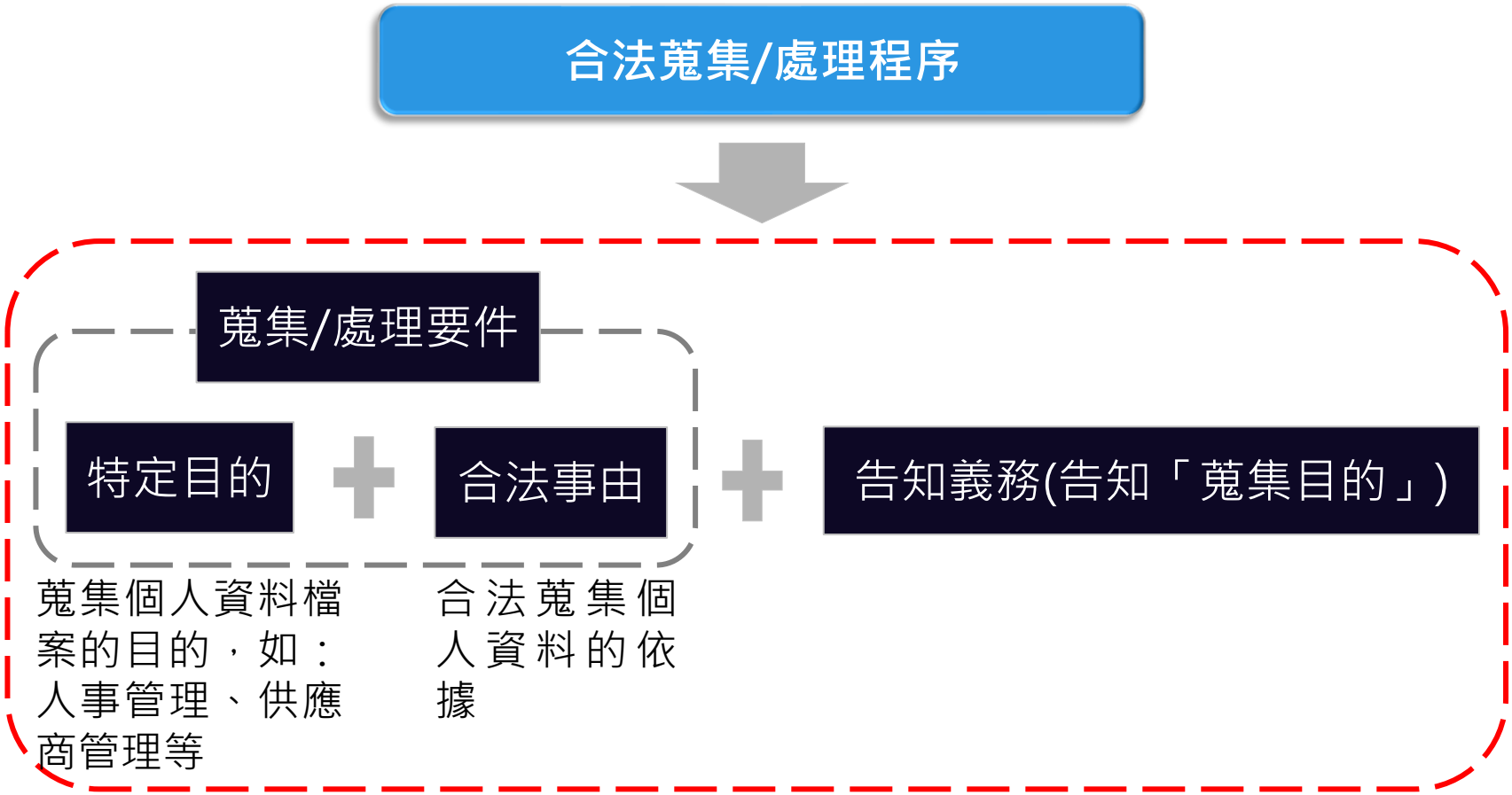
有下列情形之一者，不適用本法規定：

二、於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。

例如，於公園拍照時，無意所拍攝到路人。

不要標籤我！！！

如何合法蒐集/處理個資？



可參考法務部公告之個人資料保護法之特定目的及個人資料之類別
https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL010631#lawmenu

合法蒐集/處理

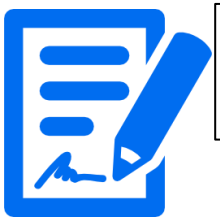
■個資法 第19條第1項

企業對個資之蒐集或處理，...，應有特定目的，並必須在符合第19條所列的情形範圍之內，方為合法(參閱合法蒐集之要求)。

■例如：

法律明文規定

勞基法第7條：雇主應建置勞工名卡



與當事人有契約或類似契約之關係，且已採取適當之安全措施

勞僱契約、採購契約

經當事人同意

不以書面為限定，但要能證明當事人同意之表示

告知義務的履行

告　　知

為了使個資的當事人能**明確知悉**其個資被蒐集、處理及利用之情形，進而決定是否提供個資，而要求**資料蒐集者**應善盡之義務

直 接 蒐 集

（向當事人蒐集時）

一、公務機關或非公務機關名稱。
二、蒐集之目的。
三、個人資料之類別。
四、個人資料利用之期間、地區、對象及方式。
五、當事人依第三條規定得行使之權利及方式。
六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

間 接 蒐 集

（處理或利用前、首次利用時併同為之）

一、個人資料的來源
二、公務機關或非公務機關名稱。
三、蒐集之目的。
四、個人資料之類別。
五、個人資料利用之期間、地區、對象及方式。
六、當事人依第三條規定得行使之權利及方式。

《告知內容》第8條：直接蒐集之免告知情形

- 有下列情形之一者，得免為前項之告知：
  一、依法律規定得免告知。
  二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
  三、告知將妨害公務機關執行法定職務。
  四、告知將妨害公共利益。
  五、當事人明知應告知之內容。
  六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

《告知內容》第9條：間接蒐集之免告知情形

- 有下列情形之一者，得免為前項之告知：
  一、如同直接蒐集之免告知事由；
  二、當事人自行公開或其他已合法公開之個人資；
  三、不能向當事人或其法定代理人為告知；
  四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供 者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限v
  五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料；

個人資料的合法處理程序

- 處理（§2）
  - ✓ 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。

- 合法處理之要求（§19 I）
  - ✓ 企業對個資之蒐集或處理，…，應有特定目的，並必須在符合第19條所列的情形範圍之內，方為合法(參閱合法蒐集之要求)。
  - ✓ 只要是在特定目的內的處理，不用另外取得當事人的同意。

「特定目的之範圍」最少要等同於「未來處理利用之範圍」

個人資料的合法利用

原　則	應於蒐集之特定目的**必要範圍內**為利用！
例　外	應符合目的外利用之**法定情形**！

- ✓ 法律明文規定
- ✓ 為增進公共利益所必要
- ✓ 免除個資當事人生命、身體、自由或財產上之危險
- ✓ 防止他人權益之重大危害
- ✓ 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，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- ✓ 經當事人同意
- ✓ 有利於當事人權益

利用個資行銷，不得不慎！

■某連鎖賣場電子郵件擾民，判賠2.6萬

■消費者向賣場行使刪除其個資，並獲同意，但仍接到52封郵件

■新法實施前，36封應賠1萬元；新法實施後寄16封，一封賠1000元，計1萬6000元。

（https://news.ltn.com.tw/news/society/breakingnews/1131420）

行　銷

- 拒絕即應停止利用其個資行銷
- 首次行銷，應提供拒絕行銷的方式，並支付所需費用

特種個資的蒐集、處理及利用

■個資法第六條

有關病歷、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、處理或利用。但符合法定情形者，不在此限：

有某些種類的個人資料，因為較為敏感，如果遭到外洩或濫用，將會產生莫大的危害！
因此**原則上是禁止蒐集、處理或利用**！

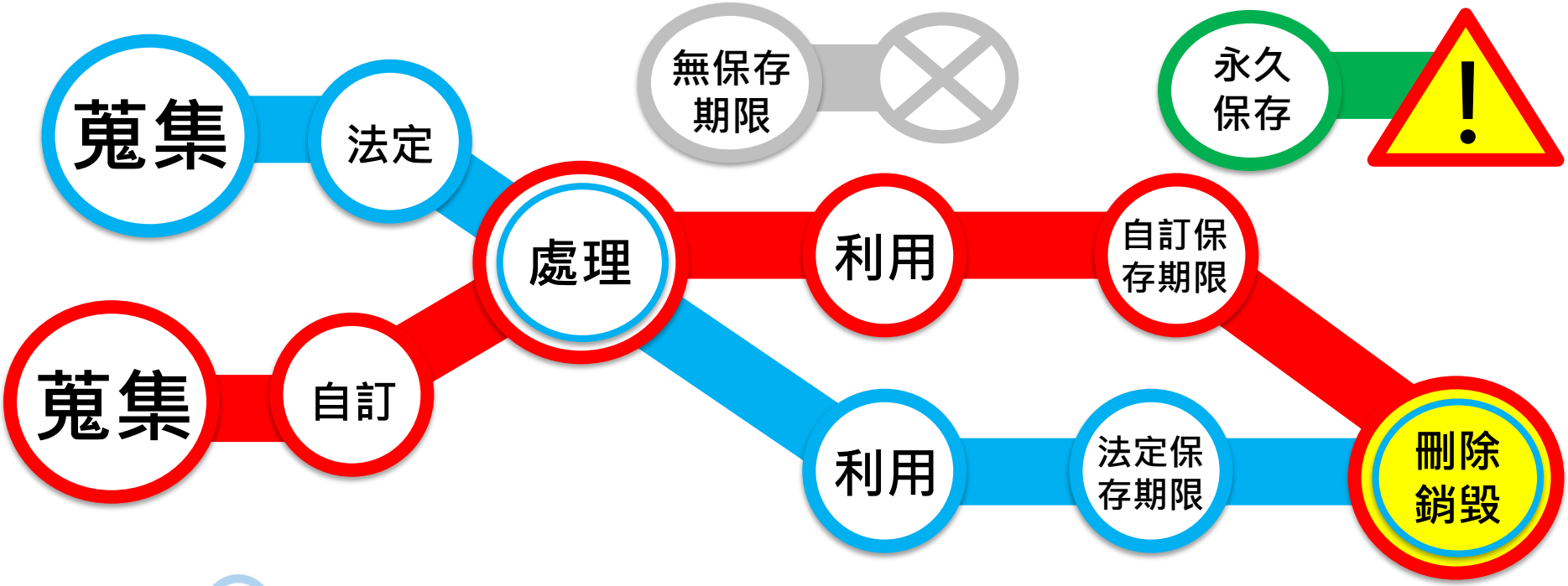
■例外得蒐集、處理及利用特種個資的法定情形

- 法律明文規定：如保險法第177-1條。
- 經當事人「書面」同意。

個人資料的合法刪除

- 應主動或依當事人之請求刪除 之情形有二：
  - ✓ 個人資料蒐集之特定目的消失或期限屆滿時(§11 Ⅲ)
    - 例外(可不刪除之情形)
      1) 執行職務或業務所必須
      2) 經當事人書面同意者
      3) 法律另有規定
  - ✓ 違法蒐集、處理或利用個資者(§11 Ⅳ)

個人資料生命週期



含有個人資料檔案之保存
紙本：保存於上鎖之區域
電子：以適當方式加密

紀錄的保留

案例分享

(2011年12月21日蘋果日報)

近來醫院病歷個資外洩層出不窮，又有XXXX醫院離職員工爆料，院方將最重要的**病歷違法擱置在地下停車場，且擺放兩年**，「真的很離譜！」對此，XXXX醫院解釋，因空間不足才暫時堆放該處，地下停車場只有醫師才能申請使用，且都有警衛巡視，故不會有個資外洩問題，但已立即移置這些病歷資料。主管機關XX縣衛生局表示，院方違反《醫療法》，可處最高5萬元罰鍰。

投訴者XX溫先生表示，曾在XXXX醫院服務，發現醫院竟將患者病歷，一箱箱放置在地下室停車場，已違法擺放兩年。

資料來源：http://www.appledaily.com.tw/appledaily/article/headline/20111221/33900741/

大綱

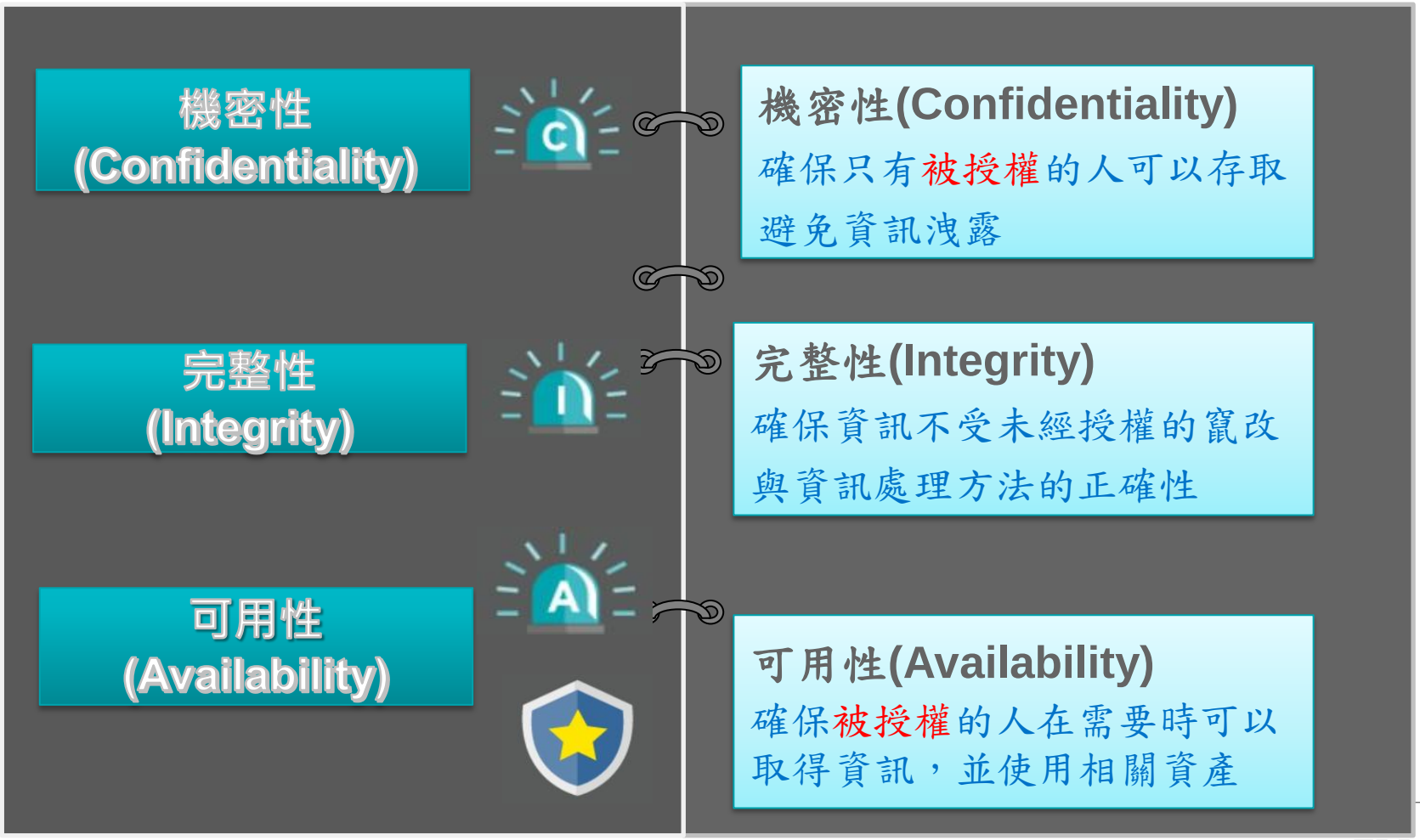
何謂資訊安全?

資訊安全是保護組織的重要資訊免遭未經授權的存取或修改，以確保其機密性、完整性和可用性

- 一個好的資訊安全管理制度可以
  - 降低威脅發生的可能
  - 降低風險
  - 確保組織業務持續性

資訊安全概念

- 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(C)，使資訊免於受到破壞(I)，影響其使用(A)。



ISO 27001:2013 資訊安全管理制度

目的

- 提供最佳資訊安全管理實務
- 讓組織能據以發展、導入、維運、以及量測資訊安全管理實務的有效性
- 讓交易雙方能因此具備信心與信任
- 適用於各種大小、業態與規模的組織

目標

- 以事前應對(proactive)、系統化(systematic)及邏輯化(logical)的方法來描述資訊安全問題

ISO 27001:2013 資訊安全管理制度

依照ISO Annex SL用於管理系統之要求，標準架構統一如下：

ISO 27001:2013 附錄A - 參考控制領域

14個領域，114個控制項

A.5 資訊安全政策

A.6 資訊安全組織

A.7 人力資源安全

A.8 資產管理

A.9 存取控制

A.10 密碼技術

A.11 實體與環境安全

A.12 作業安全

A.13 通訊安全

A.14 系統之取得、開發與維護

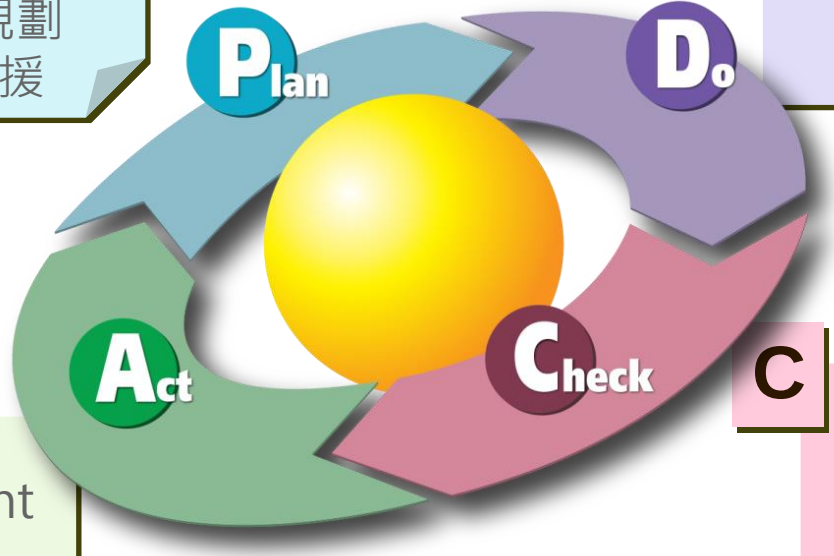
A.15 供應商管理

A.16 資訊安全事故管理

A.17 營運持續管理之資訊安全面向

A.18 符合性

資訊安全管理制度 PDCA 循環



P 建立目標

4. Context of the organization 組織環境
5. Leadership 領導
6. Planning 規劃
7. Support 支援

D 實施計畫過程

8. Operation 運作

C 監督與量測

9. Performance evaluation 績效評估

A 採取改善措施

10. Improvement 改善

ISO 27001 資訊安全管理優點

- 確保資訊安全
- 強化顧客滿意
- 提供顧客或相關人員對風險管理的信心
- 安全交換資訊
- 為組織帶來利益
- 建構資訊安全文化
- 最小風險暴露
- 保護組織資訊資產
- 以事前應對(proactive)、系統化(systematic)及邏輯化(logical)的方法來描述資訊安全問題

4. Context of the organization 組織環境

組織應

◆ 4.1 Understanding the organization and its context 瞭解組織及其環境

The Organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS

組織應決定與其目的有關且影響達成其資訊安全管理系統預期成果能力者之內部及外部議題。

◆ 4.2 Understanding the needs and expectations of interested parties

瞭解利害關係團體的需求與期望

- (a) interested parties that are relevant to ISMS
  與資訊安全管理系統有關之關注方；
- (b) the requirements of these interested parties relevant to ISMS
  關注方對資訊安全之要求事項；
- 要求事項可包含法律及法規要求，以及契約義務。

4. Context of the organization 組織環境(續)

組織應

- 4.3 Determining the scope of the information security management system
  決定資訊安全管理系統範圍
  Shall consider the external and internal issues, the requirements and interfaces and dependencies between activities perform by the organization, and those that are performed by other organizations
  應考量內外部議題(4.1)、關注方的要求事項(4.2)、組織所執行的活動，以及由其他組織執行活動間的介面與相依性。

- 4.4 Information security management system
  依據本標準要求事項，建立、實作、維護與持續改進資訊安全管理系統。

5. Leadership 領導

高階管理階層應

◆ 5.1 Leadership and commitment 領導與承諾

Demonstrate leadership and commitment with respect to the ISMS
展現對ISMS的領導與承諾

- 確保已建立資訊安全政策及資訊安全目標，並與組織之策略方向相容；
- 確保資訊安全管理系統要求事項整合入組織之各項過程；
- 確保資訊安全管理系統所需之資源可取得；
- 傳達有效之資訊安全管理的重要性，以及符合資訊安全管理系統要求事項之重要性；
- 確保資訊安全管理系統達成其預期成果；
- 指導及支援人員，以促進資訊安全管理系統之有效性；
- 推動持續改善；
- 當適用其他相關管理角色之責任範圍時，加以支持以展現其領導權。

5. Leadership 領導(續)

高階管理階層應

◆ 5.2 Policy 政策

Establish an information security policy 建立資訊安全政策

- 切合組織目標；
- 包括資訊安全目標(參照6.2)或提供設定資訊安全目標使用之框架；
- 包括對滿足相關於資訊安全之適用要求事項的承諾；
- 包括對持續改善資訊安全管理系統之承諾。

資訊安全政策應符合下列項目

- 以文件化資訊提供；
- 於全組織內傳達；
- 適用時，提供給關注方(利害相關團體)。

5. Leadership 領導(續)

高階管理階層應

◆ 5.3 Organizational roles, responsibilities and authorities

組織的角色、責任與授權

Ensure the responsibilities and authorities for roles relevant to information security are assigned and communicated

確保資安相關角色的責任與授權已指派與溝通

最高管理階層應指派下列責任及權限：

- 確保資訊安全管理系統符合本標準之要求事項；
- 向最高管理階層報告資訊安全管理系統之績效。

6. Planning 規劃

◆ 6.1 Actions to address risks and opportunities 風險與機會處理措施

6.1.1 General 概述

Ensure the ISMS can achieve its intended outcomes; prevent, or reduce, undesired effects; and achieve continual improvement
確保 ISMS 能達成預定成效，預防與降低非預期影響，並達成持續改善。

The organization shall plan actions to address these risks and opportunities, and how to

組織應規劃因應此等風險及機會之處理措施，以及執行下列事項之方法：

1) Integrate and implement the actions into its ISMS

將各項措施整合及實作於其資訊安全管理系統過程之中。

2) Evaluate the effectiveness of these actions 評估措施之有效性。

6. Planning 規劃(續)

◆ 6.1 Actions to address risks and opportunities 風險與機會處理措施

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

Define an information security risk assessment process, criteria and risk acceptance criteria
界定資訊安全風險評鑑流程、各項準則以及風險接受準則。

Ensure that repeated information security risk assessments produce consistent, valid and comparable results
確保重複執行的資訊安全風險評鑑能產生一致、有效並可比較的結果。

6. Planning 規劃(續)

◆ 6.1 Actions to address risks and opportunities 風險與機會處理措施

6.1.2 Information security risk assessment 資訊安全風險評鑑(續)

Identify information security risk 識別資訊安全風險

1) apply the information risk assessment process to identify risk associated with the loss of confidentiality, integrity, and availability for information within the scope of ISMS
應用資訊安全風險評鑑過程，以識別ISMS範圍內與資訊機密性、完整性及可用性喪失相關聯之風險。

2) Identify the risk owners 識別風險擁有者。

6. Planning 規劃(續)

◆ 6.1 Actions to address risks and opportunities 風險與機會處理措施

6.1.2 Information security risk assessment 資訊安全風險評鑑(續)

analyses an information security risk 分析資訊安全風險

1) assess the potential consequences that would result if the risks identified were to materialize

評估已識別風險可能產生的潛在結果。

2) assess the realistic likelihood of the occurrence of the risk identified

評估已識別風險發生真正的可能性。

3) determine the levels of the risk 決定風險的等級。

6. Planning 規劃(續)

◆ 6.1 Actions to address risks and opportunities 風險與機會處理措施
6.1.3 Information security risk treatment 資訊安全風險處理

Apply an information security risk treatment process
執行資訊安全風險處理流程

1) Select appropriate treatment options
考量風險評鑑結果，選擇適切的處理選項。

2) Determine all controls
對所選定資訊安全風險處理選項，決定所有必須實作之控制措施。

3) Compare the controls with Annex A
與「附錄A」控制措施比較，確認未忽略必要之 控制措施。

4) Produce a Statement of Applicability
產生適用性聲明書，包括必要之控制措施，且不論是否實作，提供納入之理由，以及由附錄A排除之理由。

6. Planning 規劃(續)

◆ 6.1 Actions to address risks and opportunities 風險與機會處理措施
6.1.3 Information security risk treatment 資訊安全風險處理

Apply an information security risk treatment process
執行資訊安全風險處理流程
5) Formulate a treatment plan 規劃資訊安全風險處理計畫。
6) Obtain risk owner's approval
取得風險擁有者對資訊安全風險處理計畫的核准，以及對剩餘資訊安全風險之接受。

6. Planning 規劃(續)

◆ 6.2 Information security objectives and plans to achieve them
資訊安全目標與達成計畫
The information security objective shall 資訊安全目標應

- Be consistent with the information security policy, measurable, communicated, updated as appropriate
  與資訊安全政策一致、可量測、被加以溝通、且適當地更新。
- Take into account applicable information security requirements, and risk assessment and treatment results
  考量資訊安全要求，以及風險評鑑與處理結果。

6. Planning 規劃(續)

◆ 6.2 Information security objectives and plans to achieve them

資訊安全目標與達成計畫(續)

When planning, the organization shall determine 規劃時，組織應決定

- What will be done (應完成之工作)；
- what resource will be required (所需資源)；
- Who will be responsible (負責人員)；
- When it will be completed (達成時間)；
- How the results will be evaluated（結果評估方式）。

7. Support 支援

◆ 7.1 Resources 資源

Determine and provide the resources needed for the ISMS

決定與提供ISMS所需資源。

◆ 7.2 Competence 能力

Shall determine and ensure the necessary competence

應決定相關人員應擁有之必要能力，並確保人員擁有之。

Ensure competence on the basis of appropriate education, training, or experience

確保此等人員於適當教育、訓練或經驗之基礎上能勝任。

Take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken

於適當時，採取取得必要能力之措施，並評估該措施之有效性。

Evidence of competence 保存適切之文件化資訊，作為勝任之證據。

7. Support 支援(續)

◆ 7.3 Awareness 認知

Persons shall be aware of the ISMS policy, their contribution to the ISMS, and the implications of not conforming with the ISMS requirements

人員應認知到資訊安全政策，對ISMS有效性的貢獻，以及未遵循ISMS要求的後果。

◆ 7.4 Communication 溝通

Determine internal and external communications needs on what, who, when, with whom, and the processes

決定內外部溝通需求，包括溝通事項、執行方式、人員、時間、對象與流程。

7. Support 支援(續)

◆ 7.5 Documented information 文件化資訊

7.5.3 Control of documented information 管理文件化資訊

Documented information shall be controlled to ensure available, suitable for use, and adequately protected

文件化資訊應被適當管理以確保可用、合適、並被加以保護(如機密性喪失、不適當利用、或完整性喪失) 。

7. Support 支援(續)

◆ 7.5 Documented information 文件化資訊

7.5.3 Control of documented information 管理文件化資訊(續)

Organization shall address documentation control

組織應於適當時，考量下列控制文件化資訊之活動:

1) distribution, access, retrieval and use 分發、存取、檢索及利用；

2) storage and preservation 儲存及保存，包含可讀性的保存；

3) control of changes 變更管制(版本控管)；

4) retention and disposition 保存及屆期處置。

於適當時，應識別及控制由組 織所決定對資訊安全管理系統之規劃及運作為必要之外部來源的文件化資訊。

8. Operation 運作

◆ 8.1 Operational planning and control 運作規劃與控制

Plan, implement and control the processes & actions
計畫、實行、以及控制流程與執行方案(6.1) 。

Implement plans to achieve information security objectives
執行計畫以達成資訊安全目標(6.2) 。

Ensure outsourced processes are determined and controlled
組織應確保委外流程加以決定與管制。

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

Perform risk assessments at planned intervals or when significant changes occur
定期或於發生重大變動時執行風險評鑑。

8. Operation 運作(續)

- 8.3 Information security risk treatment 資訊安全風險處理
  Implement the risk treatment plan 執行風險處理計畫

9. Performance evaluation 績效評估

◆ 9.1 Monitoring, measurement, analysis, and evaluation
監視、量測、分析與評估

Evaluate the information security performance and the effectiveness of the ISMS
評估資訊安全績效與 ISMS 的有效性

組織應決定下列事項:

- 需要監督及量測之事項，包括資訊安全過程及控制措施。
- 監督、量測、分析及評估之適用方法，以確保有效的結果。所選擇之方法宜產生可比較及可重製，以確認其有效。
- 執行監督及量測之時機。
- 監督及量測之人員。
- 監督及量測結果應分析及評估之時間。
- 分析及評估上述結果之人員。

9. Performance evaluation 績效評估(續)

◆ 9.2 Internal audit 內部稽核

Conduct internal audits at planned intervals to provide information on whether the ISMS：

定期執行內部稽核以確認ISMS是否：

- Conforms to the requirements of this international Standard and the organization

  符合本標準與組織之要求。

- Is effectively implemented and maintained

  被有效的實作與維護。

9. Performance evaluation 績效評估(續)

◆ 9.2 Internal audit 內部稽核

組織應採取下列作為:

1) 規劃、建立、實作及維持稽核計畫，包括頻率、方法、責任、規劃要求事項及 報告。該稽核計畫應將所關注之重要流程及前次稽核之結果納入考量；

2) 定義各稽核之準則及稽核之範圍；

3) 選擇稽核員及施行稽核，以確保稽核過程之客觀性及公平性；

4) 確保稽核之結果對相關管理階層報告；

5) 保存文件化資訊作為稽核計畫及稽核結果之證據。

9. Performance evaluation 績效評估(續)

◆ 9.2 Internal audit 內部稽核

內部稽核用來幫助偵測可疑的行為，有下列三個目標:

- 確保所有的運作均能按照既定的安全政策執行。
- 確保所有資料的存取都要經過授權。
- 確保所有資料的正確性。

透過內部稽核活動，以了解組織是否達到下列要求:

- 符合國際標準或法規要求。
- 符合所辨識出之資訊安全要求。
- 有效執行並持續維護。
- 如預期般執行。

9. Performance evaluation 績效評估(續)

◆ 9.3 Management review 管理審查

Top management shall review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness

高階管理階層應定期審查組織ISMS以持續確保適切性、合適性與有效性

- 前次管理審查所決議之行動方案的執行狀態；
- 與ISMS相關的內外部議題變更；
- 資訊安全績效的回饋，包含不符合項目及矯正措施、監督及量測結果、稽核結果、資訊安全目標之達成；
- 利害相關團體回饋；
- 風險評鑑結果與風險處理計畫狀態；
- 持續改善的機會。

9. Performance evaluation 績效評估(續)

◆ 9.3 Management review 管理審查(續)

Top management shall review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness
高階管理階層應定期審查組織ISMS以持續確保適切性、合適性與有效性

- 前次管理審查所決議之行動方案的執行狀態；
- 與ISMS相關的內外部議題變更；
- 資訊安全績效的回饋，包含不符合項目及矯正措施、監督及量測結果、稽核結果、資訊安全目標之達成；
- 利害相關團體回饋；
- 風險評鑑結果與風險處理計畫狀態；
- 持續改善的機會。

管理審查的輸出項目應包含資訊安全管理系統持續改善機會與變更需求的決策；

10. Improvement 改善

◆ 10.1 Nonconformity and corrective action 不符合事項與矯正措施

組織應

- React to the nonconformity

  因應不符合事項。採取措施控制及矯正，並處理其後果。

- Evaluate the need for action to eliminate the causes of nonconformity

  評估執行行動，審查並決定不符合原因，以消除不符合事項原因之需求。

- Implement any action needed 執行所需措施。
- Review the effectiveness of any corrective action taken

  審查矯正措施有效性。

- Make changes to the ISMS 對 ISMS 進行變更。

10. Improvement 改善

◆ 10.2 Continual improvement 持續改善

The organization shall continually improve the suitability, adequacy, and effectiveness of the ISMS

組織應持續改善ISMS的適切性、合適性、與有效性。

Q & A