照過來～比黑五採購秘笈還厲害的，不看你會後悔

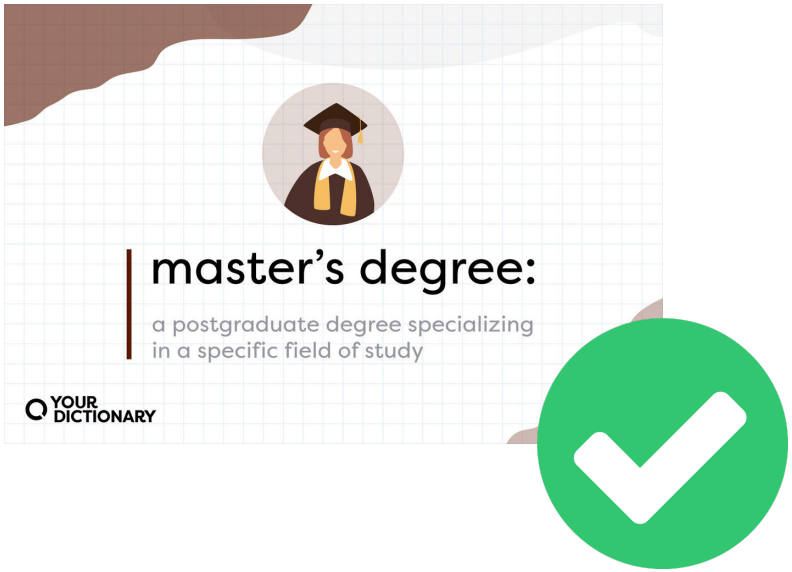
Edward Lin

2023/12/14

自我介紹

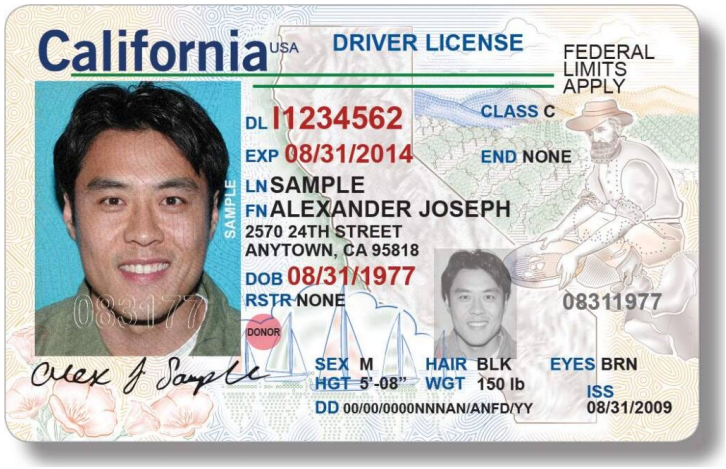
描述：
暮光之城 無懼的愛 電影海報
來源：
http://www.spp.com.tw/spp2006/other/07/twilight/news.htm
日期：
2009.2.14
作者：
尖端出版

So plz call me Edward (aka 愛德華)



Why I am in here ?

秘笈？規範？

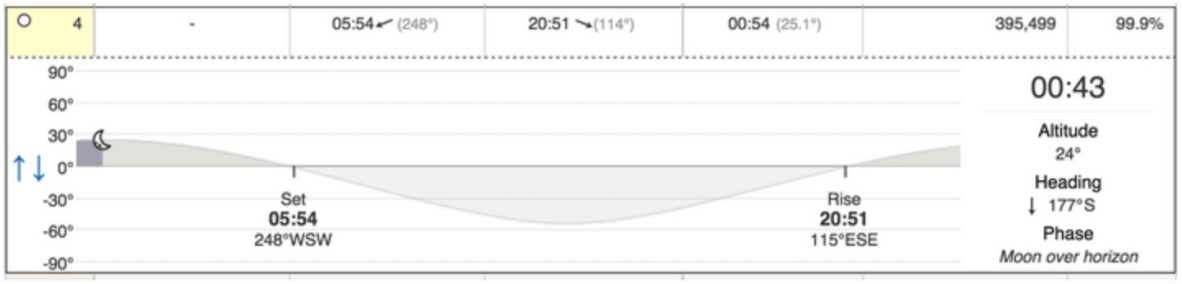

California USA
DRIVER LICENSE
FEDERAL LIMITS APPLY
DL I1234562
CLASS C
EXP 08/31/2014
END NONE
LN SAMPLE
FN ALEXANDER JOSEPH
2570 24TH STREET
ANYTOWN, CA 95818
DOB 08/31/1977
RSTR NONE
08311977
DONOR
SEX M
HAIR BLK
EYES BRN
HGT 5'-08"
WGT 150 lb
ISS 08/31/2009
DD 00/00/0000NNNAN/ANFD/YY
SAMPLE


STOP
Stop
Give Way
One Way
No Entry
One Way
One Way Both Direction
Right Turn Prohibited
Left Turn Prohibited
Mandatory Signs
bankbazaar.com
One Way
U-Turn Prohibited
Over Taking Prohibited
Horns Prohibited
65 Km/h
Speed Limit
Compulsory Turn Left
Compulsory Ahead Only
Compulsory Turn Right Ahead
Compulsory Ahead Or Turn Right
Compulsory Ahead Or Turn Left
Compulsory Keep Left
Compulsory Sound Horn

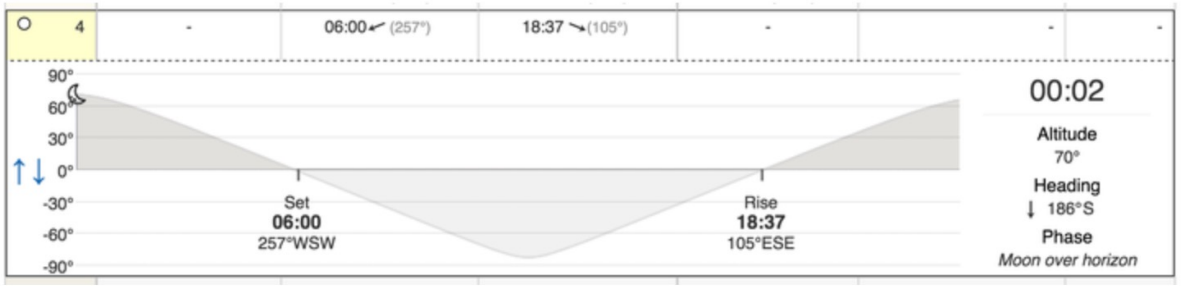
外國月亮比較大比較圓？

倫敦的月亮高度約為24°，而阿克拉的月亮高度為70°。

倫敦人看月亮會感覺離高樓更近一些，所以視覺上感覺更大。



圖一：倫敦



圖二：阿克拉

規範？法律？傻傻分不清

ISO International Organization for Standardization

PCI Security Standards Council
PARTICIPATING ORGANIZATION™

NIST National Institute of Standards and Technology

GDPR

金融資安行動方案2.0 - 精進重點

項次	推動措施	擴大適用	落實深化	鼓勵前瞻
1	擴大資安長設置，定期召開**資安長聯繫會議**	V	V	◎
2	因應數位轉型及及網路服務開放，增修訂自律規範		V	
3	深化**核心資料保全**及營運持續演練		V	V
4	擴大導入國際資安管理標準及建置資安監控機制	V	V	
5	鼓勵資安監控與防護之**有效性評估**		V	V
6	鼓勵**零信任網路部署**，強化連線驗證與授權管控			V
7	鼓勵配置多元專長資安人才，擴大**攻防演訓**量能		V	V
8	提升資安情資分享動能，增進資安聯防運作效能		V	
9	辦理資安攻防演練，規劃**重大資安事件支援演訓**		V	

臺灣資通安全管理法的架構

資通安全管理法（母法）
- 資通安全管理法施行細則（子法）
- 資通安全責任等級分級辦法（子法）
- 資通安全情資分享辦法（子法）
- 資通安事件通報及應變辦法（子法）
- 特定非公務機關資通安全維護計畫（子法）
- 公務機關所屬人員辦理資通安全業務獎懲辦法（子法）

資料來源：iThome整理，2018年5月

個資法

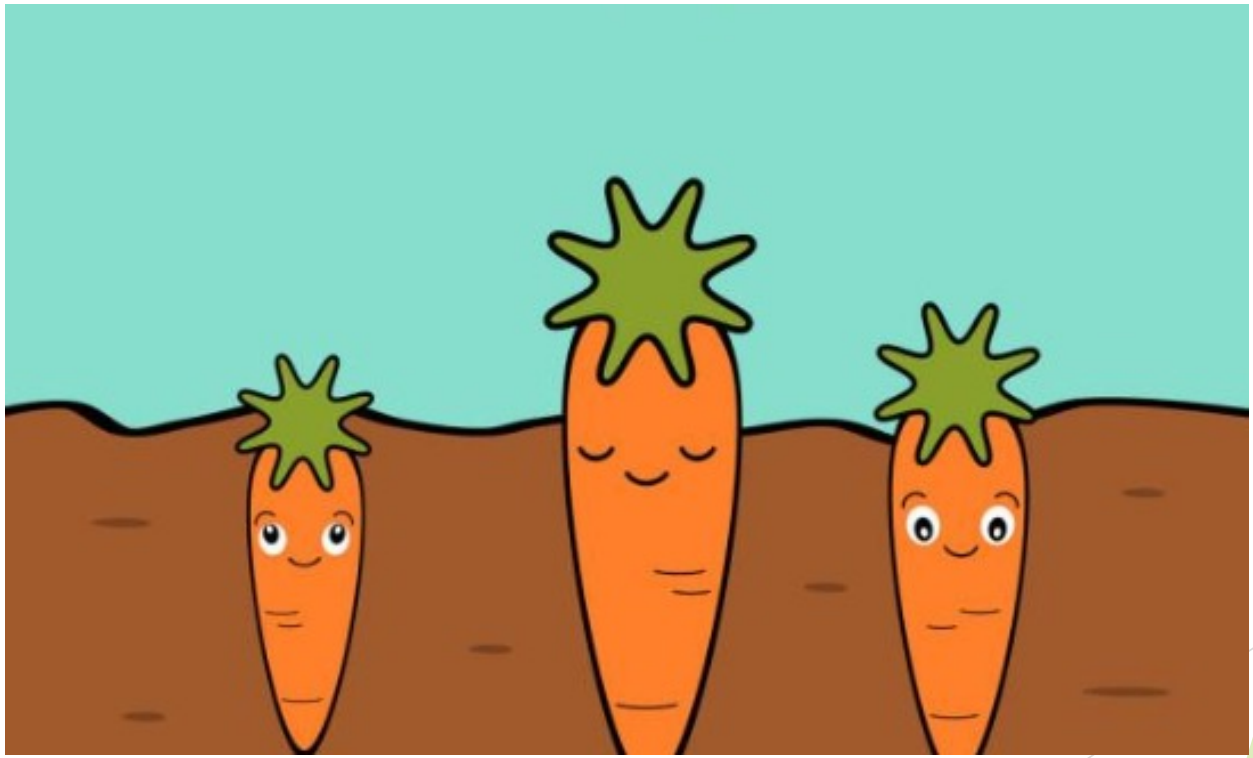
總則	第 1 條～第 14 條 用詞定義、當事人權利、委外、蒐集、處理、利用、書面同意、告知義務、個資維護
公務機關對個人資料的蒐集、處理、利用	第 15 條～第 18 條 蒐集、處理、利用的要件、個人資料檔案公開、安全維護義務
非公務機關對個人資料的蒐集、處理、利用	第 19 條～第 27 條 蒐集、處理、利用的要件、國際傳輸、行政檢查、安全維護義務
損害賠償與團體訴訟	第 28 條～第 40 條 民事賠償責任、團體訴訟
罰則	第 41 條～第 50 條 刑事責任、行政處罰
附則	第 51 條～第 56 條 例外情形、其他規定

iThome

所以呢？秘笈是？

- 因人而異、因地制宜
- 小處著眼、處處著手
- 做個快樂傻 D

因人而異、因地制宜（I）



因人而異、因地制宜（II）@ 台灣篇

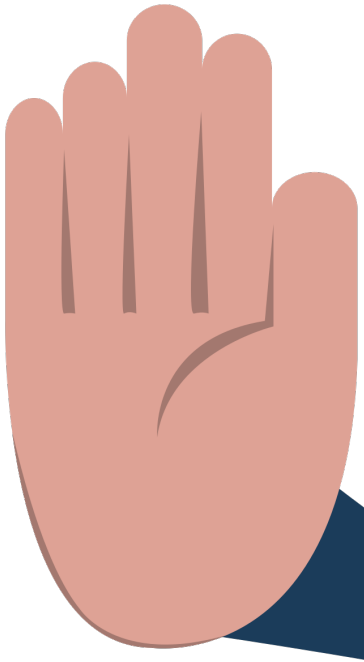
小處著眼、處處著手


防 詐 騙
重要提醒
夏普震旦不會以任何形式主動向顧客索取金融帳戶資料，也不會要求您前往提款機操作匯款與分期事宜。如接獲可疑電話，請立即撥打[165防詐騙專線]，請保持警覺，切勿上當。
— 防詐騙 三不原則 —
不隨便 提供個人資料
不理會 來路不明電話
不聽從 他人指示操作ATM
警政署反詐騙專線：165
警政署全民防騙網：165.npa.gov.tw

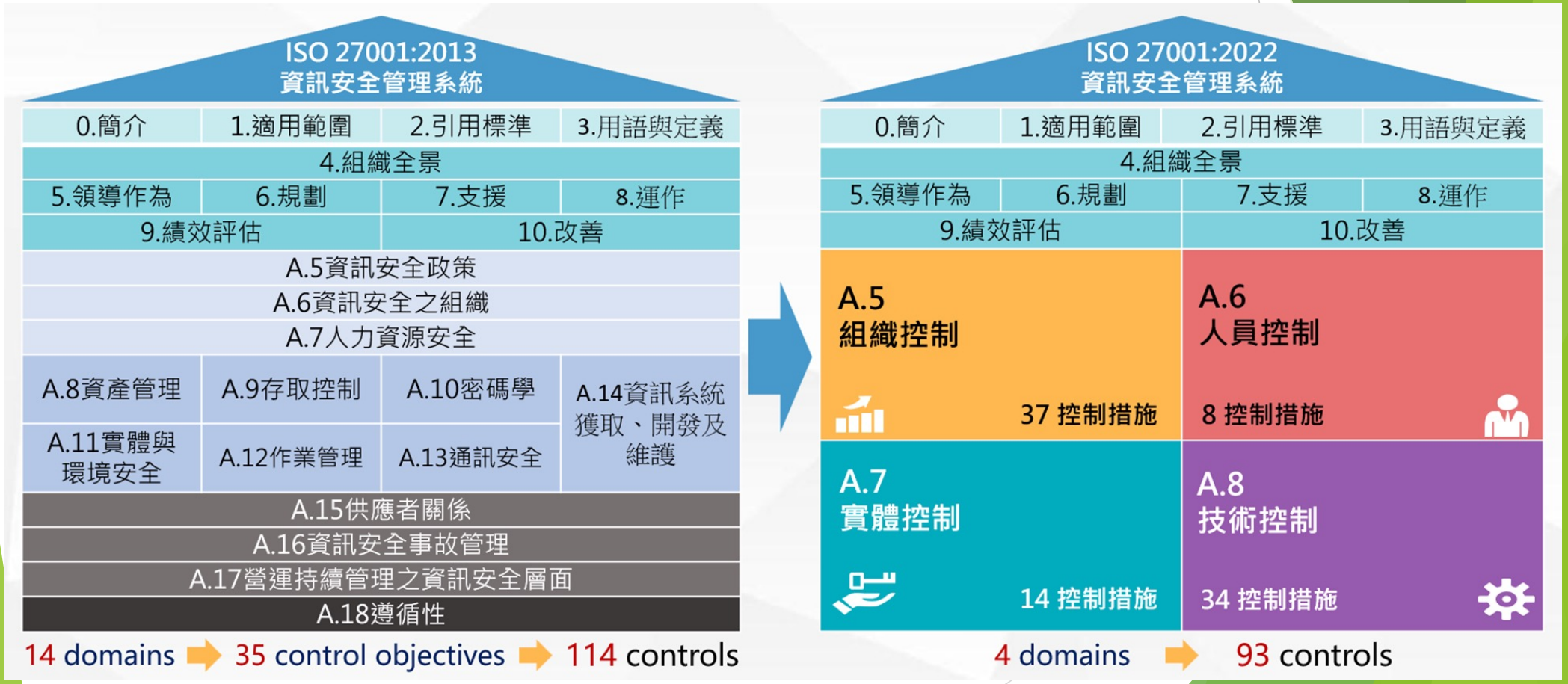

常見詐騙手法！
STORE
網購詐騙
一頁式廣告
來路不明的購物網站
假求職詐騙
提供財產資料
提供存摺、印章、金融卡
假公務機關詐騙
要求匯款
監管帳戶
網戀詐騙
虛擬世界的愛情陷阱
比你想像中多！
假電信業者詐騙
提供個人資訊
簡訊或來電通知繳費
假投資詐騙
高倍快速獲利
獨聽不賠
165
反詐騙
165APP
共同反詐騙
whos call
whoscall
過濾不明電話
雲林縣警察局關心您
廣告

快樂做個傻 D

- 凡事先以 No 為基礎
- 天底下沒有白吃的午餐
- 「拒絕」為唯一的王道！
- 沒知識要有常識，沒常識要常看「書」



講這麼多，到底秘笈長怎樣？



2022 年武功秘笈新增項目

- 威脅情報
- 雲服務的資訊安全
- 業務持續準備 @ ICT 產業
- 實體安全監控
- 組態管理
- 資訊資料刪除
- 資訊資料屏蔽
- 預防資訊洩漏
- 監控活動
- 網頁過濾
- 安全程式編碼

武功秘笈基本功 (I)

- 定義驗證範圍
- 確認負責人與相關人員職責
- 制定資安目標以及組織資安原則

武功秘笈基本功（II）

- 進行資訊資產盤點與分級
  - 很重要、很重要、很重要（很重要所以說三次）
  - 資訊資產不是僅是「電腦」、「伺服器」
- 進行人員角色與職責盤點與確認
  - 很重要、很重要、很重要（很重要所以說三次）
  - 不是 IT 人員才是要盤點與確認的人

武功秘笈基本功（III）

- 依據範圍與組織資安目標，並遵從秘笈指示
  - 制定相關對應準則、手冊以及規範內容
- 全部以 CIA 為最高衡量指標
- 並符合 AAA 之目標要求

武功秘笈基本功（IV）

- 文件機密等級分類
  - 一般、敏感、機密
- ISO 文件分類
  - 第一階文件 - 政策、適用性聲明
  - 第二階文件 - 程序書
  - 第三階文件 - 說明書
  - 第四階文件 - 空白表單、紀錄及其他

武功秘笈基本功（V）

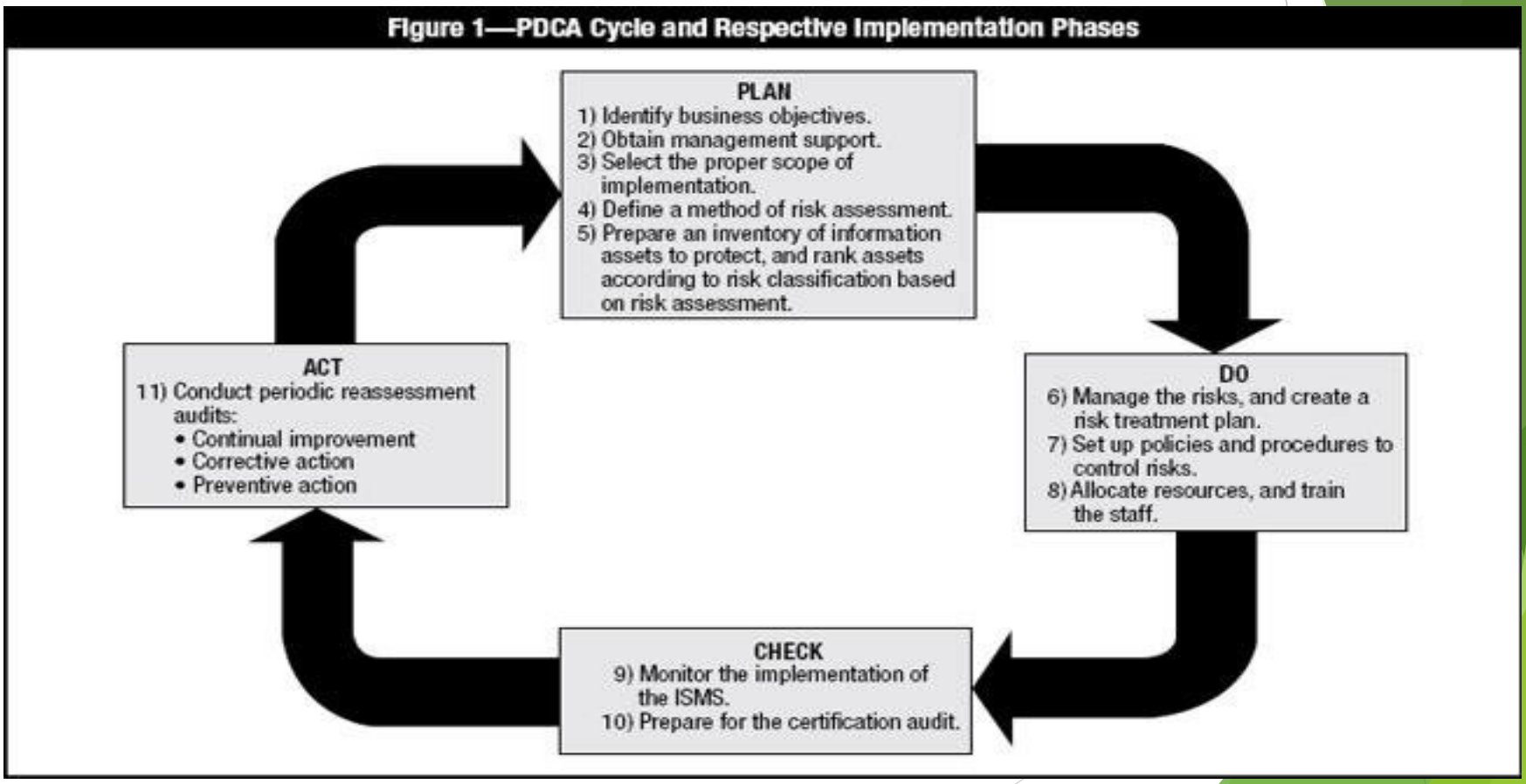
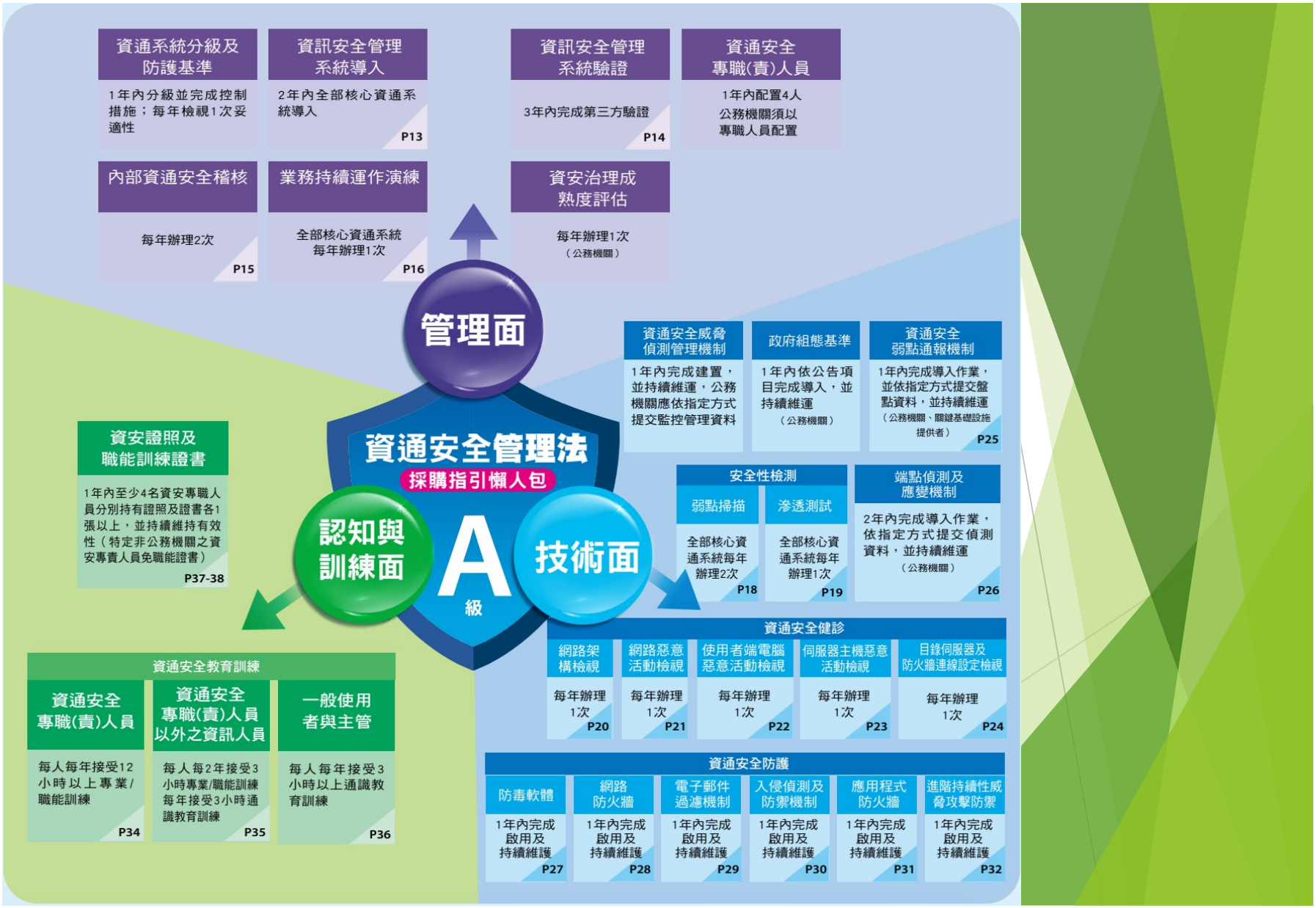


Figure 1—PDCA Cycle and Respective Implementation Phases
PLAN
1) Identify business objectives.
2) Obtain management support.
3) Select the proper scope of implementation.
4) Define a method of risk assessment.
5) Prepare an inventory of information assets to protect, and rank assets according to risk classification based on risk assessment.
DO
6) Manage the risks, and create a risk treatment plan.
7) Set up policies and procedures to control risks.
8) Allocate resources, and train the staff.
CHECK
9) Monitor the implementation of the ISMS.
10) Prepare for the certification audit.
ACT
11) Conduct periodic reassessment audits:
• Continual improvement
• Corrective action
• Preventive action


資通系統分級及防護基準
1年內分級並完成控制措施；每年檢視1次妥適性
資訊安全管理系統導入
2年內全部核心資通系統導入
P13
資訊安全管理系統驗證
3年內完成第三方驗證
P14
資通安全專職(責)人員
1年內配置4人
公務機關須以專職人員配置
內部資通安全稽核
每年辦理2次
P15
業務持續運作演練
全部核心資通系統每年辦理1次
P16
資安治理成熟度評估
每年辦理1次
（公務機關）
管理面
資通安全管理法
採購指引懶人包
A級
認知與訓練面
技術面
資通安全威脅偵測管理機制
1年內完成建置，並持續維運，公務機關應依指定方式提交監控管理資料
政府組態基準
1年內依公告項目完成導入，並持續維運
（公務機關）
資通安全弱點通報機制
1年內完成導入作業，並依指定方式提交盤點資料，並持續維運
（公務機關、關鍵基礎設施提供者）
P25
資安證照及職能訓練證書
1年內至少4名資安專職人員分別持有證照及證書各1張以上，並持續維持有效性（特定非公務機關之資安專責人員免職能證書）
P37-38
安全性檢測
弱點掃描
全部核心資通系統每年辦理2次
P18
滲透測試
全部核心資通系統每年辦理1次
P19
端點偵測及應變機制
2年內完成導入作業，依指定方式提交偵測資料，並持續維運
（公務機關）
P26
資通安全健診
網路架構檢視
每年辦理1次
P20
網路惡意活動檢視
每年辦理1次
P21
使用者端電腦惡意活動檢視
每年辦理1次
P22
伺服器主機惡意活動檢視
每年辦理1次
P23
目錄伺服器及防火牆連線設定檢視
每年辦理1次
P24
資通安全教育訓練
資通安全專職(責)人員
每人每年接受12小時以上專業/職能訓練
P34
資通安全專職(責)人員以外之資訊人員
每人每2年接受3小時專業/職能訓練
每年接受3小時通識教育訓練
P35
一般使用者與主管
每人每年接受3小時以上通識教育訓練
P36
資通安全防護
防毒軟體
1年內完成啟用及持續維護
P27
網路防火牆
1年內完成啟用及持續維護
P28
電子郵件過濾機制
1年內完成啟用及持續維護
P29
入侵偵測及防禦機制
1年內完成啟用及持續維護
P30
應用程式防火牆
1年內完成啟用及持續維護
P31
進階持續性威脅攻擊防禦
1年內完成啟用及持續維護
P32

Q & A (I)

- Q1：外國月亮比較圓，是指哪一國？

Q & A (II)

- Q2：以下哪一個不屬於資安範疇？
  - 筆電
  - 伺服器
  - 不斷電系統
  - 監視器
  - 「隔壁小王」

Q & A (III)

- Q3：紙本沒有通電，所以不是資安範疇？對或錯

Q & A (IV)

- Q4：ISO 9000、ISO 20000、ISO 27001 哪一個是資安標準？

Q&A(V)

- Q5：資安最大秘笈是？
  - 當個傻D(Deny)
  - 當原始人(所有資訊設備都不用)
  - 立志讓我的電腦變成為毒窟就是萬能
  - 人生有幾回，一回生二回熟。多被騙幾次，我就是人生勝利組