教育體系資通安全與個資保護管理規範

鍾沛原 專案經理

成大資通安全研究與教學中心

2020/10/27

大綱

- 管理規範架構
- 管理規範本文
- 管理規範附錄A
- 結論

管理規範架構

管理規範發展

- 初版(中華民國96年5月30日版)
  - ISO/IEC 27001:2005
  - 行政院及所屬各機關資訊安全管理規範
- 二版(中華民國105年8月5日版)
  - ISO/IEC 27001:2013
  - BS 10012:2009
- 三版(中華民國109年9月9日版)
  - ISO/IEC 27001:2013
  - BS 10012:2017 & ISO 29100:2011 &ISO 29151:2017

適用範圍

- 資通安全責任等級非屬A、B 級之教育體系機關（構）與各級學校
  - ISMS：應至少包含資訊管理單位、學術網路系統、核心資通系統。
  - PIMS：應至少包含涉及核心業務之個人資料蒐集、處理與利用流程之行政單位，以及資訊管理單位。

備註：欲建立「資通安全暨個人資料管理系統」之機關（構）與學校，得分別定義兩項管理系統之適用範圍，惟PIMS 適用範圍所涉及之資通安全管理議題，應完整包含於ISMS 之適用範圍內。

適用性聲明

- 本文(柒、建置步驟及需求)
  - 不可排除
- 附錄A
  - 控制措施之排除僅限適用範圍內資訊系統無需執行，且排除後不影響該單位提供資通安全能力與責任之控制措施。
  - 教育機構如欲取得驗證，所有附錄A 資訊安全管理規範內之控制項，除標註「建議」者外，均應納入，同時應參考「資通安全責任等級分級辦法」附表九資通系統防護需求分級原則，鑑別適用範圍內資訊系統之安全等級，經資訊系統分級與鑑別後，識別出具有等級為「高」者之資訊系統，應加入A.14 系統獲取、開發及維護控制領域所有控制措施，並於該控制措施中述明適用之資訊系統。

適用性聲明(cont.)

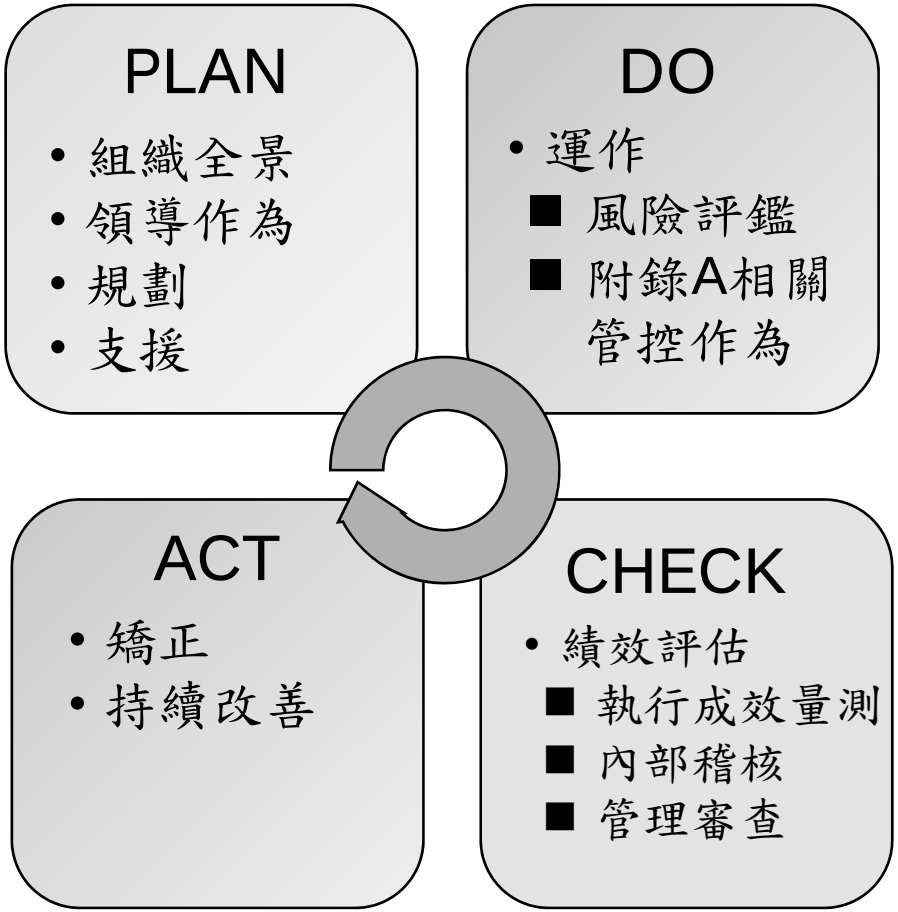
- 附錄B
  - 擬建置PIMS 之機關（構）與學校，應選用附錄B 中所有非屬「建議」之控制項，另可依據實施狀況選擇標註「建議」之控制項。

資通系統防護需求分級原則

防護需求等級 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資 通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷， 對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致 資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

管理規範本文

PDCA


PLAN
• 組織全景
• 領導作為
• 規劃
• 支援
DO
• 運作
■ 風險評鑑
■ 附錄A相關管控作為
CHECK
• 績效評估
■ 執行成效量測
■ 內部稽核
■ 管理審查
ACT
• 矯正
• 持續改善

本文條款(cont.)

- 組織全景(Plan)
  - 建立或調整資通訊安全與個人資訊管理範圍與目標
  - 利害相關團體與要求事項
  - 上述事項之定期審查(每年至少一次)

資通安全維護計畫

- 核心業務即重要性
  - 核心業務
  - 核心資通系統
  - 重要性說明
  - 業務失效影響說明
  - 最大可容忍中斷時間
- 非核心業務
  - 業務失效影響說明
  - 最大可容忍中斷時間
- 機關資通安全責任等級分級

本文條款(cont.)

- 領導作為(Plan)
  - 領導及承諾
    - 建立或核定機關（構）或學校之管理政策與目標。
    - 傳達管理制度要求事項之遵循與持續改善的承諾。
    - 提供管理制度運行所需資源及人力。

資通安全維護計畫
- 資通安全政策
- 資通安全目標
  - 量化型目標
  - 質化性目標
- 資通安全政策及目標之核定程序
- 資通安全政策及目標之宣導
- 資通安全政策及目標定期檢討程序

本文條款(cont.)

- 建立政策與目標
  - 管理政策文件化，向內部及利害相關團體公告或傳達
  - 包含資訊安全目標與持續改善之承諾
  - 管理審查政策與目標，配合變更需求予以修訂

資通安全維護計畫
- 資通安全政策
- 資通安全目標
  - 量化型目標
  - 質化性目標
- 資通安全政策及目標之核定程序
- 資通安全政策及目標之宣導
- 資通安全政策及目標定期檢討程序

本文條款(cont.)

- 指派角色、責任及權限
  - 建立制度管理小組，指派人員並賦予其管理之責任與權限，定期（每年至少一次）或於重大變更時向管理階層報告管理制度執行成效。

資通安全維護計畫
- 資通安全長
- 資通安全推動小組
  - 組織
  - 分工執掌
    - 策略規劃組
    - 資安防護組
    - 績效管理組
- 專職(責)人力資源之配置

本文條款(cont.)

- 規劃(Plan)
  - 管理目標達成風險與機會之因應行動
  - 建立風險管理程序
    - 建立與維持風險準則
    - 識別、分析並評估風險
      - 機密性、完整性、可用性與適法性
    - 選擇風險處理措施
    - 產生或評估適用性聲明書(資訊安全風險處理使用)
    - 制訂風險處理計畫並取得核准

資通安全維護計畫
- 資通安全風險評估
  - 針對資訊及資通系統資產進行風險評估
  - 核心資通系統之辨識、標示及最大可容忍中斷時間
- 資通安全風險之因應

風險評鑑範例

項次	資產名稱	類別	擁有者/職稱	機密性©	完整性(I)	可用性(A)	資訊資產價值(T)(C,I,A取最大值)	潛在風險事件	風險發生可能性(V)	風險值 資訊資產價值*(T*V)
1.	EVO派送軟體	軟體資產	資訊教師	1	1	3	3	1.3.2	2	6
2.	個人電腦	實體資產	全體教職員	1	1	2	2	2.3.3	2	4
3.	行動裝置	實體資產	全體教職員	1	1	1	1	2.4.3	2	2
4.	可攜式媒體	實體資產	全體教職員	1	1	1	1	2.5.2	2	2
5.	學校網站	軟體資產	資訊教師	1	1	1	1	1.2.2	1	1

風險類型暨風險對策參考表

資產大類	資產小類	潛在風險事件	管控措施範例說明
1. 軟體資產類	1. 1 作業系統	1. 1. 1 未落實作業系統更新/漏洞修補，致使遭受惡意攻擊、資料外洩或其他侵害。	-WSUS 機制失效 -定期檢查漏洞更新狀態 -資訊單位定期彙整提供發佈更新資訊(，供業務單位進行比對
1. 軟體資產類	1. 1 作業系統	1. 1. 2 未購買妥適的作業系統授權/使用授權超過購買數，致使遭受廠商求償或抗議。	-作業系統授權清單
1. 軟體資產類	1. 1 作業系統	1. 1. 3 未汰換原廠公告停止技術支援之作業系統，進而無法修補漏洞，致使遭受惡意攻擊、資料外洩或其他侵害。	
1. 軟體資產類	1. 1 作業系統	1. 1. 4 未加入組織之網域，進而無法套用 GCB 或群組原則政策，致使無法有效管控。	-套用 GCB 設定，或設定適當權組原則
1. 軟體資產類	1. 1 作業系統	1. 1. 5 個人電腦或伺服器等資訊設備，未安裝適當之防毒軟體或安全防護軟體，於網路連線時遭電腦病毒入侵或被植入惡意程式，致使資料外洩或遭受其他侵害。	

本文條款(cont.)

- 管理目標及其達成之規劃
  - 相關執行活動或事項
  - 所需投入之人員、預算、設備技術與程序表單等資源
  - 活動或事項負責人員
  - 活動或事項預計完成時間
  - 管理目標是否達成之評估方式**(可量測)**

資通安全維護計畫
- 資通安全政策
- 資通安全目標
  - 量化型目標
  - 質化性目標
- 資通安全政策及目標之核定程序
- 資通安全政策及目標之宣導
- 資通安全政策及目標定期檢討程序

本文條款(cont.)

- 支援(Plan)
  - 資源
  - 能力
  - 認知
  - 文件化資訊

資通安全維護計畫
- 專職(責)人力資源之配置
- 經費之配置
- 資通安全教育訓練要求
- 資通安全教育訓練辦理方式

本文條款(cont.)

- 運作(Do)
  - 運作之規劃及控制
  - 執行風險評鑑
  - 實作風險處理

資通安全維護計畫
- 資通安全維護計畫之實施
- 資通安全風險評估
  - 針對資訊及資通系統資產進行風險評估
  - 核心資通系統之辨識、標示及最大可容忍中斷時間
- 資通安全風險之因應

本文條款(cont.)

- 績效評估(Check)
  - 監督、量測、分析及評估
    - 需要監督及量測之事項
    - 監督、量測、分析及評估之適用方法
    - 執行監督及量測的時間
    - 監督及量測的人員
    - 監督及量測結果之分析及評估時間
    - 分析及評估上述結果之人員

資通安全維護計畫
- 資通安全維護計畫之稽核機制
  - 稽核機制之實施
- 資通安全維護計畫之持續精進及績效管理
- 資通安全維護計畫實施情形之提出

本文條款(cont.)

- 內部稽核
  - 是否遵循組織及標準對ISMS要求之事項
  - 是否有效實做及維持
  - 規劃、建立、實作及維持稽核計畫
  - 定義各稽核之準則及稽核範圍
  - 選擇稽核員及施行稽核，確保稽核過程客觀性及公平性
  - 確保稽核結果對相關管理階層報告
  - 保存文件化資訊作為稽核計畫及稽核結果之證據

資通安全維護計畫
- 資通安全維護計畫之稽核機制
  - 稽核機制之實施
- 資通安全維護計畫實施情形之提出

本文條款(cont.)

- 管理審查
  - 過往管理審查之議案處理狀態
  - ISMS有關內外部議題的變更
  - 資訊安全績效之回饋，包括不符合項目及矯正措施、監督及量測結果、稽核結果、資訊安全目標達成
  - 關注方之回饋
  - 風險評鑑結果及風險處理計畫之狀態
  - 持續改善之機會

資通安全維護計畫

- 資通安全維護計畫之稽核機制
  - 稽核改善報告
- 資通安全維護計畫之持續精進及績效管理
- 資通安全維護計畫實施情形之提出

本文條款(cont.)

- 改善(Act)
  - 不符合項目及矯正措施
    - 對不符合項目反應，包括採取適當行動以矯正之、處理其後果
    - 評估對消除不符合項目之原因的行動需要，使其不再發生且不於他處發生
    - 實作所有所需行動
    - 審查所有採取矯正措施之有效性
    - 必要時進行ISMS變更
  - 持續改善
    - 持續改善管理制度的合宜性、適切性及有效性

資通安全維護計畫
- 資通安全維護計畫之持續精進及績效管理
- 資通安全維護計畫實施情形之提出

管理規範附錄A

A.5 資訊安全政策

- A.5.1 資訊安全之管理指導方針
  - A.5.1.1 資訊安全政策(I/P)
    - 資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。
  - A.5.1.2 資訊安全政策之審查(I/P)
    - 資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。

資通安全維護計畫
- 資通安全政策及目標之核定程序
- 資通安全政策及目標之宣導
- 資通安全政策及目標定期檢討程序

A.6 資訊安全組織

- A.6.1 內部組織
  - A.6.1.1 資訊安全之角色及責任(I/P)
  - A.6.1.2 職務區隔
  - A.6.1.3 與權責機關之聯繫
  - A.6.1.4 與特殊關注方之聯繫
  - A.6.1.5 專案管理之資訊安全(建議)
    - 不論專案之型式，應在專案管理中因應資訊安全。

資通安全維護計畫
- 資通安全長
- 資通安全推動小組
  - 組織
  - 分工執掌
    - 策略規劃組
    - 資安防護組
    - 績效管理組
- 專職(責)人力資源之配置
- 資通安全情資之分類評估

A.6.1.5 專案管理之資訊安全

- 對於有完成時間之資訊相關專案，如資訊系統發展、維護或升級專案、軟硬體購置或升級專案等，宜考量在專案管理之資訊安全，如：

(1)將資訊安全目標涵蓋於專案目標內。

(2)在專案的初期階段實施資訊安全風險評鑑以識別必要的控制措施。

(3)資訊安全要求事項納入專案各階段管理作業。

(4)在所有專案中宜每階段或專案變更前處理與審查資訊安全相關議題。

(5)在專案管理方法中宜對特定角色界定與賦予資訊安全責任。

A.6 資訊安全組織

- A.6.2 行動裝置及遠距工作
  - A.6.2.1 行動裝置政策
    - 應採用政策及支援之安全措施，以管理因使用行動裝置所導致之風險。
  - A.6.2.2遠距工作
    - 應實作政策及支援之安全措施，以保護存取、處理或儲存於遠距工作場所之資訊。

資通安全維護計畫
- 作業與通訊安全管理
  - 遠距工作之安全措施
  - 行動設備之安全管理

A.6.2.1 行動裝置政策

- 資通安全維護計畫
  - 機密資料不得由未經許可之行動設備 存取、處理或傳送。
  - 機敏會議或場所不得攜帶未經許可之行動設備。
  - 其餘可參考 其餘可參考 參考 CNS 27002 編號 6.2.1 行動裝置政策 行動裝置政策 、政府行動化安全防護規劃報告行動裝置資安防護參考指引

A.7 人力資源安全

- A.7.1 聘用前
  - A.7.1.1 篩選(I/P)
  - A.7.1.2 聘用條款及條件(I/P)
- A.7.2 聘用期間
  - A.7.2.1 管理階層責任(I/P)
  - A.7.2.2 資訊安全認知、教育及訓練(I/P)
    - 施行單位內所有員工及相關之承包者，均應接受及其工作職務相關的組織政策及程序之適切認知、教育及訓練，並定期更新。
  - A.7.2.3 懲處過程

資通安全維護計畫

- 資通安全教育訓練要求
- 資通安全教育訓練辦理方式
- 公務機關所屬人員辦理業務涉及資通安全事項之考核機制

A.7 人力資源安全(cont.)

- A.7.3 聘用之終止及變更
  - A.7.3.1 聘用責任之終止或變更(I/P)
    - 對於離調職員工傳達資訊安全要求事項與法律責任仍應持續遵守，並儘可能包括所有保密協議或聘用條款與條件中所包含的責任，且在結束聘用關係後宜持續一段期間。

A.8 資產管理

- A.8.1 資產責任
  - A.8.1.1 資產清冊(I/P)
  - A.8.1.2 資產擁有權
    - 清冊中所維持之資產應有擁有者。
  - A.8.1.3 資產之可被接受使用
  - A.8.1.4 資產之歸還
- A.8.2 資訊分級
  - A.8.2.1 資訊之分級(I/P)
  - A.8.2.2 資訊之標示(I/P)
  - A.8.2.3 資訊之處置(I/P)

資通安全維護計畫
- 資訊及資通系統盤點
  - 辦理資訊及資通系統資產盤點
  - 資訊及資通系統資產項目
- 機關資通安全責任等級分級
- 資訊及資通系統之管理
  - 資訊及資通系統之保管
  - 資訊及資通系統之使用
- 作業與通訊安全管理
  - 媒體防護措施
  - 電腦使用之安全管理

A.8 資產管理(cont.)

- A.8.3 媒體處置
  - A.8.3.1 可移除式媒體之管理(I/P)
  - A.8.3.2 媒體之汰除(I/P)
  - A.8.3.3 實體媒體傳送(I/P)

資通安全維護計畫
- 資訊及資通系統之管理
  - 資訊及資通系統之使用
  - 資訊及資通系統之刪除或汰除

A.9 存取控制

- A.9.1 存取控制之營運要求事項
  - A.9.1.1 存取控制政策(I/P)
  - A.9.1.2 對網路及網路服務之存取
- A.9.2 使用者存取管理
  - A.9.2.1 使用者註冊及註銷(I/P)
  - A.9.2.2 使用者存取權限之配置(I/P)(建議)
  - A.9.2.3 具特殊存取權限之管理(I/P)
  - A.9.2.4 使用者之秘密鑑別資訊的使用(I/P)
    - 應以正式之管理過程控制秘密鑑別資訊的配置。
  - A.9.2.5 使用者存取權限之審查(I/P)
  - A.9.2.6 存取權限之移除或調整(I/P)

資通安全維護計畫

- 存取控制與加密機制管理
  - 網路安全控管
  - 資通系統權限管理
  - 特權帳號之存取管理

A.9 存取控制(cont.)

- 應建立用於驗證使用者身分的秘密鑑別資訊（如通行碼、加密金鑰或憑證資訊等）之管理制度。秘密鑑別資訊之控管宜考量：
  - 盡量以簽訂書面約定或其他方式，要求使用者善盡保護個人通行碼之責任；如屬於群組軟體之使用者，宜確保工作群組的通行碼，僅限群組成員使用。
  - 如由使用者自行保管或維護秘密鑑別資訊(如通行碼)的機密性，宜以配予臨時性秘密鑑別資訊(如通行碼)並強迫使用者立即更改的方式處理。
  - 使用者遺失或忘記秘密鑑別資訊時，可於驗證使用者身分後，提供臨時性的通行碼，以利系統辨認使用者。
  - 宜以安全的方式將臨時的秘密鑑別資訊(如通行碼)交付使用者，避免經由第三者，或是以未受保護的電子郵遞等電子方式交付給使用者，並建立確認收到之機制。
  - 系統如經評估須建立更高等級的安全機制，可利用電子簽章等安全等級更高的存取控制技術。

A.9 存取控制(cont.)

- A.9.3 使用者責任
  - A.9.3.1 秘密鑑別資訊之使用(I/P)
    - 於使用秘密鑑別資訊時，應要求使用者遵循施行單位之實務規定。
- A.9.4 系統及應用存取控制
  - A.9.4.1 資訊存取限制(I/P)
  - A.9.4.2 保全登入程序(I/P)
  - A.9.4.3 通行碼管理系統(I/P)
    - 通行碼管理系統應為互動式， 並應確保嚴謹通行碼。
  - A.9.4.4 具特殊權限功用程式之使用
  - A.9.4.5 對程式碼之存取控制

資通安全維護計畫

- 存取控制與加密機制管理
  - 網路安全控管
  - 資通系統權限管理
  - 特權帳號之存取管理

A.9 存取控制(cont.)

- 施行單位於使用秘密鑑別資訊（如通行碼、加密金鑰或憑證資訊等）時，應要求使用者遵循單位之規定。
  - 維持秘密鑑別資訊的機密性，確保不洩露給包括授權人員的任何一方。
  - 避免保留秘密鑑別資訊的紀錄（例如：在紙張、軟體檔案或手持裝置），除非其能被安全地存放，且該存放方式經過核准（例如：密碼庫）。
  - 只要秘密鑑別資訊有可能遭受破解的跡象，宜立即更改。
  - 選用嚴謹的秘密鑑別資訊，具有足夠長的最短長度（宜至少八碼，英數字混合）。
  - 不要與他人共用個人的秘密鑑別資訊。
  - 自動登入程序中內含秘密鑑別資訊做為機密鑑別資訊並儲存時，宜確保適當地保護通行碼。
  - 公務與非公務使用目的勿使用相同秘密鑑別資訊。

A.10 密碼學

- A.10.1 密碼式控制措施
  - A.10.1.1 使用密碼式控制措施之政策(I/P)
    - 應發展及實作政策，關於資訊保護之密碼式控制措施的使用。
  - A.10.1.2 金鑰管理(建議)
    - 應加以發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。

資通安全維護計畫
- 存取控制與加密機制管理
  - 加密管理

A.11 實體及環境安全

- A.11.1 保全區域
  - A.11.1.1 實體安全週界(I/P)
  - A.11.1.2 實體進入控制措施(I/P)
  - A.11.1.3 保全之辦公室、房間及設施
    - 應設計資訊處理設施所在區域之實體安全並施行之。
  - A.11.1.4 防範外部及環境威脅
  - A.11.1.5 於保全區域內工作
    - 應設計及施行資訊處理設施所在區域內工作之程序。
  - A.11.1.6 交付及裝卸區(建議)

資通安全維護計畫
- 作業與通訊安全管理
  - 確保實體與環境安全措施

A.11 實體及環境安全(cont.)

- A.11.2 設備
  - A.11.2.1 設備安置及保護(I/P)
  - A.11.2.2 支援之公用服務事業
  - A.11.2.3 佈纜安全
  - A.11.2.4 設備維護
  - A.11.2.5 資產之攜出(I/P)
  - A.11.2.6 場所外設備及資產之安全
  - A.11.2.7 設備汰除或再使用之保全(I/P)
  - A.11.2.8 無人看管之使用者設備(建議)
  - A.11.2.9 桌面淨空及螢幕淨空政策

資通安全維護計畫

- 作業與通訊安全管理
  - 確保實體與環境安全措施
  - 電腦使用之安全管理
  - 行動設備之安全管理

A.12 運作安全

- A.12.1 運作程序及責任
  - A.12.1.1 文件化運作程序
  - A.12.1.2 變更管理(I/P)
  - A.12.1.3 容量管理
  - A.12.1.4 開發、測試及運作環境之隔離
- A.12.2 防範惡意程式
  - A.12.2.1 防範惡意軟體之控制措施(I/P)
- A.12.3 備份
  - A.12.3.1 資訊備份(I/P)
    - 應依議定之備份政策， 定期取得資訊、軟體及系統的影像檔備份複本，並測試之。

資通安全維護計畫
- 作業與通訊安全管理
  - 防範惡意軟體之控制措施
  - 資料備份
  - 電腦使用之安全管理
- 資通安全防護設備
- 資通安全情資之分類評估
- 資通安全健診

A.12 運作安全(cont.)

- A.12.4 存取及監視
  - A.12.4.1 事件存錄(I/P)
  - A.12.4.2 日誌資訊之保護(I/P)
    - 應防範存錄設施及日誌資訊遭竄改及未經授權存取。
  - A.12.4.3 管理者及操作者日誌(I/P)
  - A.12.4.4 鐘訊同步
    - 組織或安全領域內所有相關資訊處理系統之鐘訊， 應與單一參考時間源同步。
- A.12.5 運作中軟體之控制
  - A.12.5.1 對運作中系統之軟體安裝
    - 應實作各項程序，以控制對運作中系統之軟體安裝。

資通安全維護計畫

- 資通安全情資之分類評估
  - 資通安全相關之訊息情資
  - 入侵攻擊情資
  - 敏感性之情資
  - 涉及核心業務、核心資通系統之情資

A.12 運作安全(cont.)

- A.12.6 技術脆弱性管理
  - A.12.6.1 技術脆弱性管理
  - A.12.6.2 對軟體安裝之限制(建議)
- A.12.7 資訊系統稽核考量
  - A.12.7.1 資訊系統稽核控制措施
    - 應仔細規劃並議定，涉及運作中系統之稽核要求事項及活動，以使營運過程中斷降至最低。

資通安全維護計畫
- 檢測項目
  - 網站安全弱點掃描
  - 系統滲透測試
- 資通安全健診

A.13 通訊安全

- A.13.1 網路安全管理
  - A.13.1.1 網路控制措施
  - A.13.1.2 網路服務之安全
  - A.13.1.3 網路之區隔
- A.13.2 資訊傳送
  - A.13.2.1 資訊傳送政策及程序(I/P)
  - A.13.2.2 資訊傳送協議(I/P)
  - A.13.2.3 電子傳訊(I/P)
  - A.13.2.4 機密性或保密協議(I/P)

資通安全維護計畫
- 作業與通訊安全管理
  - 即時通訊軟體之安全管理
- 資通安全健診
- 資通安全防護設備
- 資通安全情資之分類評估

A.14 系統獲取、開發及維護

- A.14.1 系統資訊之安全要求事項
  - A.14.1.1 資訊安全要求事項分析及規格(I/P)
    - 資訊安全相關要求，應納入新資訊系統或既有資訊系統之強化的要求事項中。
  - A.14.1.2 保全公共網路之應用服務
    - 應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。
  - A.14.1.3 保護應用服務交易(建議)
    - 應保護應用服務交易中涉及之資訊， 以防止不完整的傳輸、誤選路（mis-routing），未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。

A.14 系統獲取、開發及維護(cont.)

- A.14.2 於開發及支援過程中之安全
  - A.14.2.1 保全開發政策(建議)
  - A.14.2.2 系統變更控制程序
  - A.14.2.3 運作平台變更後，應用之技術審查
  - A.14.2.4 軟體套件變更之限制
  - A.14.2.5 保全系統工程原則
  - A.14.2.6 保全開發環境(建議)
  - A.14.2.7 委外開發
  - A.14.2.8 系統安全測試(I/P)
  - A.14.2.9 系統驗收測試(I/P)
- A.14.3. 測試資料
  - A.14.3.1 測試資料之保護(I/P)

資通安全維護計畫
- 系統獲取、開發及維護
- 檢測項目
  - 網站安全弱點掃描
  - 系統滲透測試

A.14 系統獲取、開發及維護(cont.)

- 系統之測試資料須予以保護與控管。關於系統測試資料：
  - 宜保護及控制測試資料，避免以含有個人資料的真實資料庫進行測試；如需應用真實資料，宜於事前將足以辨識個人的資料去除。
  - 使用真實資料進行測試時宜：
    - 確保適用在實際作業系統的存取控制措施，亦適用在測試用系統。
    - 真實資料被複製到測試系統時，宜依複製作業的性質及內容，在取得授權後始能進行。
    - 測試完畢後，真實資料宜立即從測試系統中刪除。真實資料的複製情形宜予以記錄，以備日後稽核之用。

A.15 供應者關係

- A.15.1 供應者關係中之資訊安全
  - A.15.1.1 供應者關係之資訊安全政策(I/P)
    - 應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。
  - A.15.1.2 於供應者協議中闡明安全性(I/P)
    - 應與每個可能存取、處理、儲存或傳達資訊，或提供IT基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。
  - A.15.1.3 資訊及通訊技術供應鏈(I/P)
- A.15.2 供應者服務交付管理
  - A.15.2.1 供應者服務之監視及審查(I/P)
  - A.15.2.2 管理供應者服務之變更(I/P)

資通安全維護計畫

- 系統獲取、開發及維護
- 檢測項目
  - 網站安全弱點掃描
  - 系統滲透測試
- 資通系統或服務委外辦理之管理
  - 選任受託者應注意事項
  - 監督受託者資通安全維護情形應注意事項

A.15 供應者關係(cont.)

- 資通安全管理法施行細則第四條
  - 一、受託者辦理業務之相關程序及環境，應具備完善之資通安全管理措施或過第三方驗證。
  - 二、受託者應配置充足且經適當之資格訓練擁有資通安全專業證照或具有類似務經驗之資通安全專業人員。
  - 五、受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

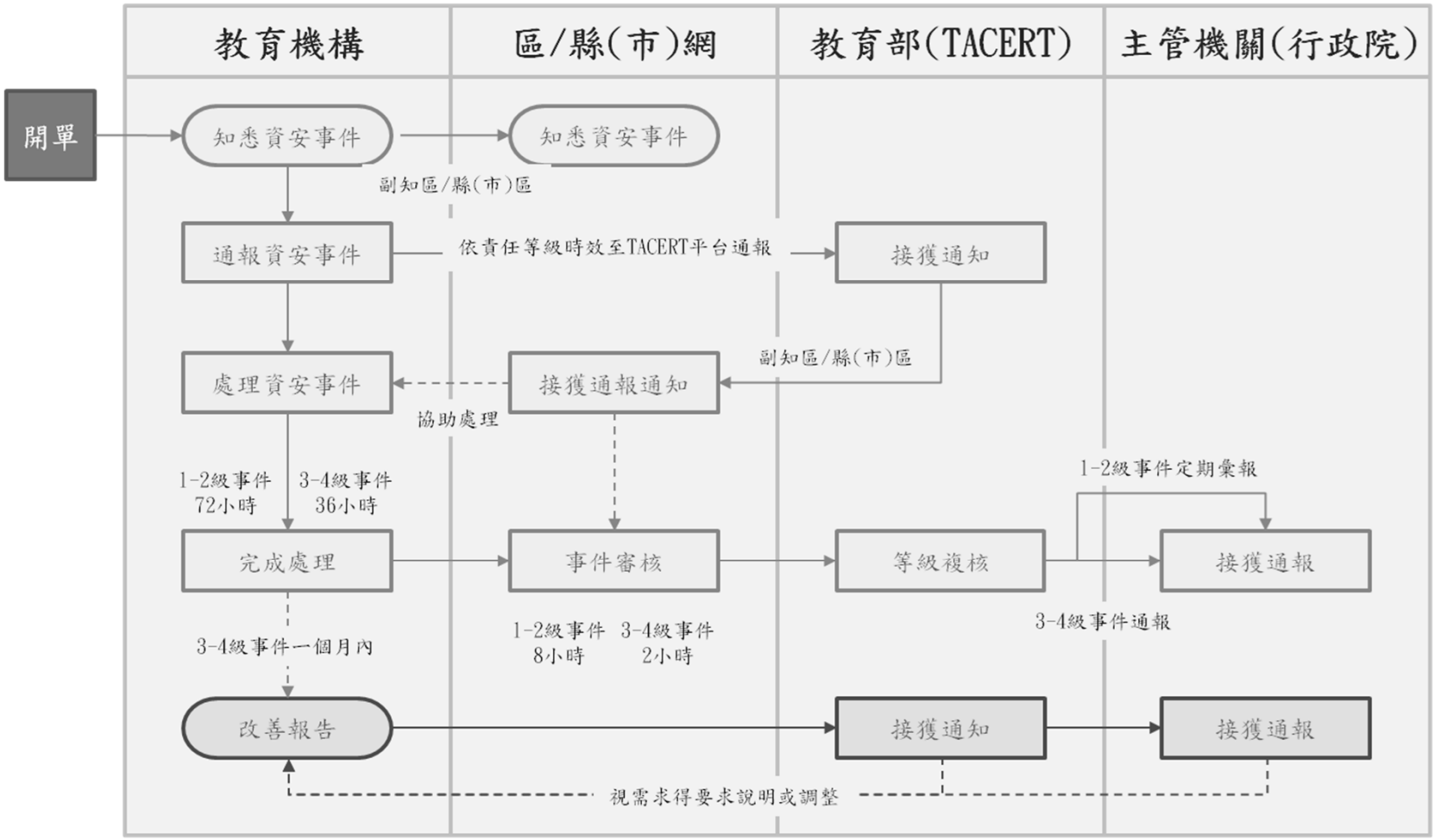
A.16 資訊安全事故管理

- A.16.1 資訊安全事故及改善之管理
  - A.16.1.1 責任及程序(I/P)
  - A.16.1.2 通報資訊安全事件(I/P)
  - A.16.1.3 通報資訊安全弱點(I/P)
  - A.16.1.4 對資訊安全事件之評鑑及決策(I/P)
  - A.16.1.5 對資訊安全事故之回應(I/P)
  - A.16.1.6 由資訊安全事故中學習(I/P)
  - A.16.1.7 證據之蒐集(I/P)

資通安全維護計畫

- 資通安全事件通報、應變及演練
- 資通安全情資之分類評估
- 資通安全情資之因應措施

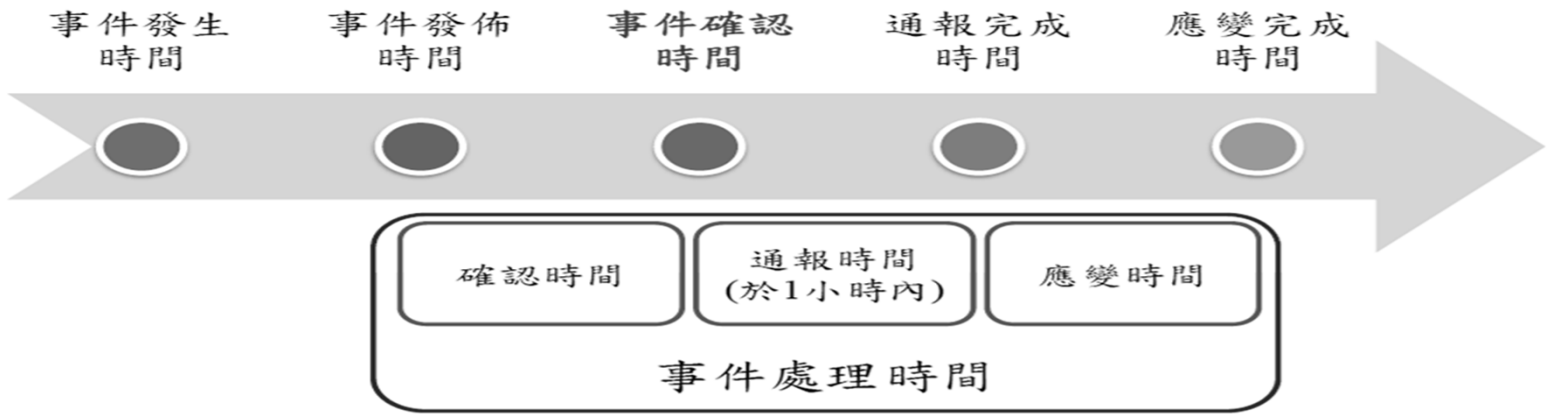
通報及應變作業流程


教育機構
區/縣(市)網
教育部(TACERT)
主管機關(行政院)
開單
知悉資安事件
知悉資安事件
副知區/縣(市)區
通報資安事件
依責任等級時效至TACERT平台通報
接獲通知
副知區/縣(市)區
處理資安事件
接獲通報通知
協助處理
1-2級事件 72小時
3-4級事件 36小時
1-2級事件定期彙報
完成處理
事件審核
等級複核
接獲通報
3-4級事件通報
1-2級事件 8小時
3-4級事件 2小時
3-4級事件一個月內
改善報告
接獲通知
接獲通報
視需求得要求說明或調整

通報及應變作業流程(cont.)

臺灣學術網路各級學校資通安全通報應變作業程序

- 依據臺灣學術網路各級學校資通安全通報應變作業程序第三章第一節第二條規定：
  - 各連線單位發現資安事件後可先進行事件確認，經確認為資安事件後，須於**一小時**內，至通報應變網站通報登錄資安事件細節、影響等級及是否申請支援等資訊，並評估該事件是否影響其他連線單位運作。



A.17 營運持續管理之資訊安全層面

- A.17.1 資訊安全持續
  - A.17.1.1 規劃資訊安全持續
  - A.17.1.2 實作資訊安全持續
  - A.17.1.3 查證、審查並評估資訊安全持續
- A.17.2 多重備援
  - A.17.2.1 資訊處理設施之可用性

資通安全維護計畫
- 資通安全事件通報、應變及演練

A.18遵循性

- A.18.1 對法律及契約要求事項之遵循
  - A.18.1.1 適用之法規及契約的要求事項之識別(I/P)
  - A.18.1.2 智慧財產權
  - A.18.1.3 紀錄之保護(I/P)
  - A.18.1.4 個人可識別資訊之隱私及保護(I/P)
  - A.18.1.5 密碼式控制措施之監管(建議)
    - 應使用密碼式控制措施(加密控制措施)，以遵循所有相關的協議、法律及法規。
- A.18.2 資訊安全審查
  - A.18.2.1 資訊安全之獨立審查(I/P)
  - A.18.2.2 安全政策及標準之遵循(I/P)
  - A.18.2.3 技術遵循審查(I/P)

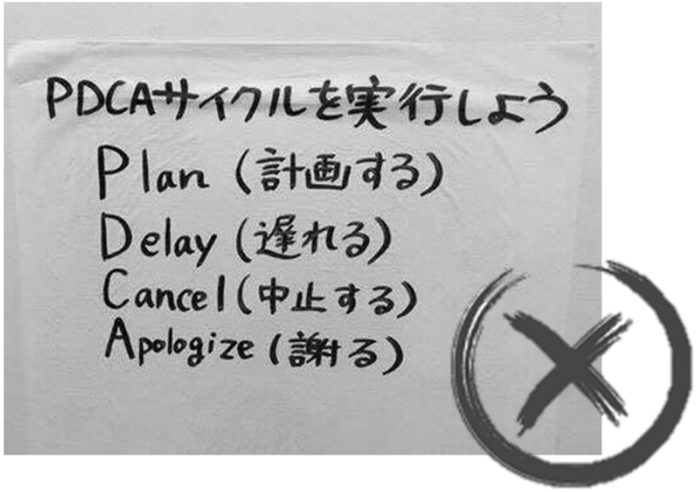
資通安全維護計畫
- 檢測項目
  - 網站安全弱點掃描
  - 系統滲透測試
- 資通安全健診

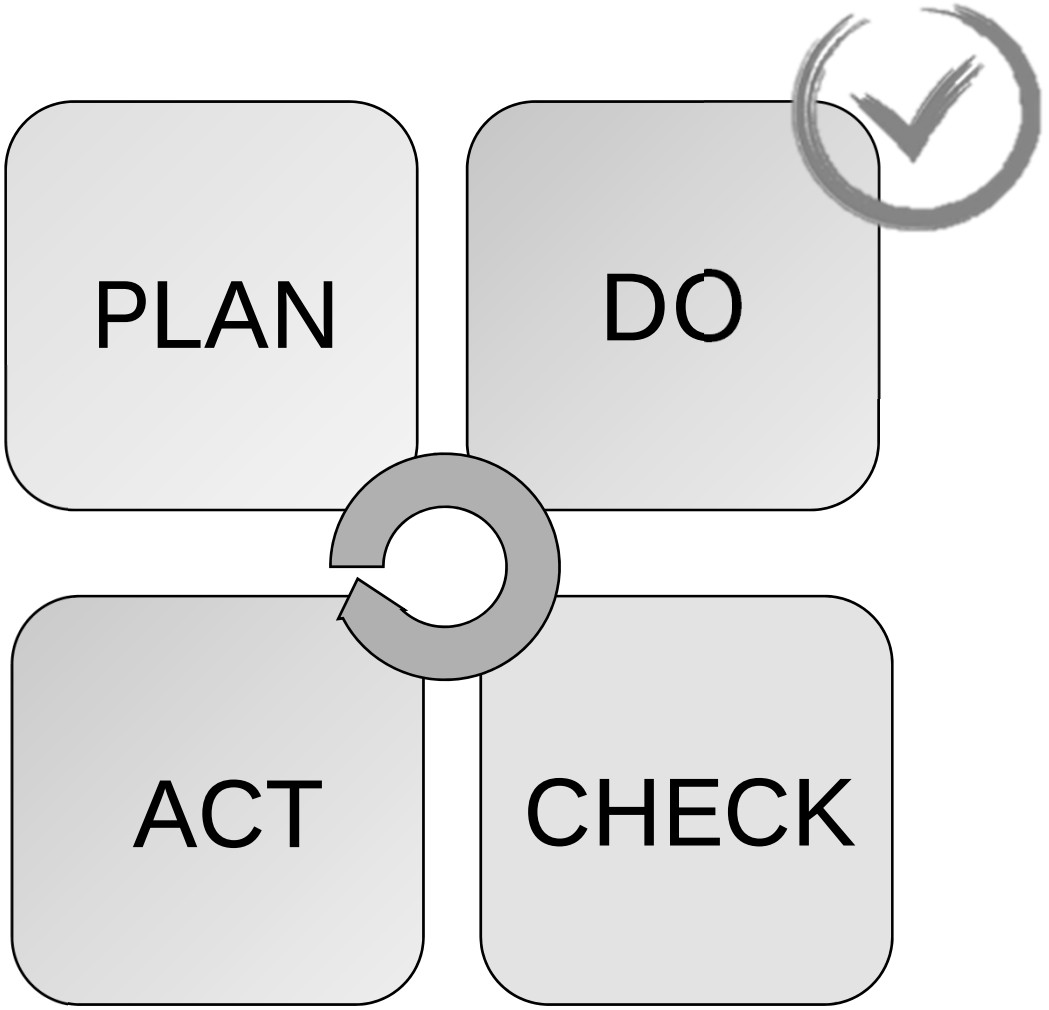
A.18遵循性(cont.)

- 應使用密碼式控制措施(加密控制措施)，以遵循所有相關的協議、法律及法規。
  - 為了遵循相關的協議、法律及法規，宜考量對加密的使用設限制，如通行碼長度、通行碼複雜度、通行碼變更週期。
  - 對外採購加密技術時，宜請廠商提供輸出國核發之輸出許可文件，並避免採購國外金鑰代管或金鑰回復之產品。

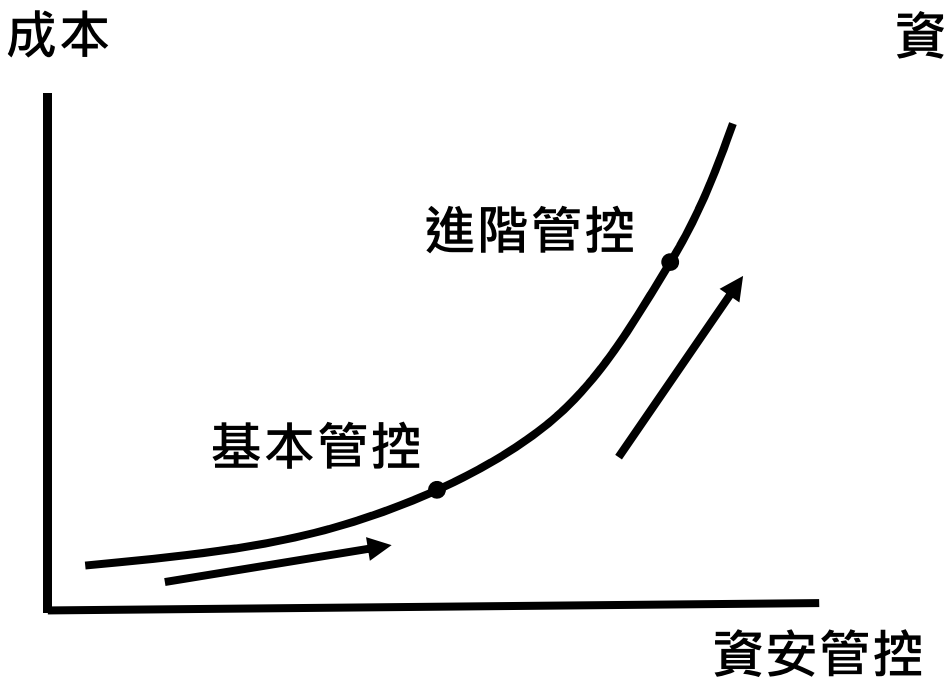
結論

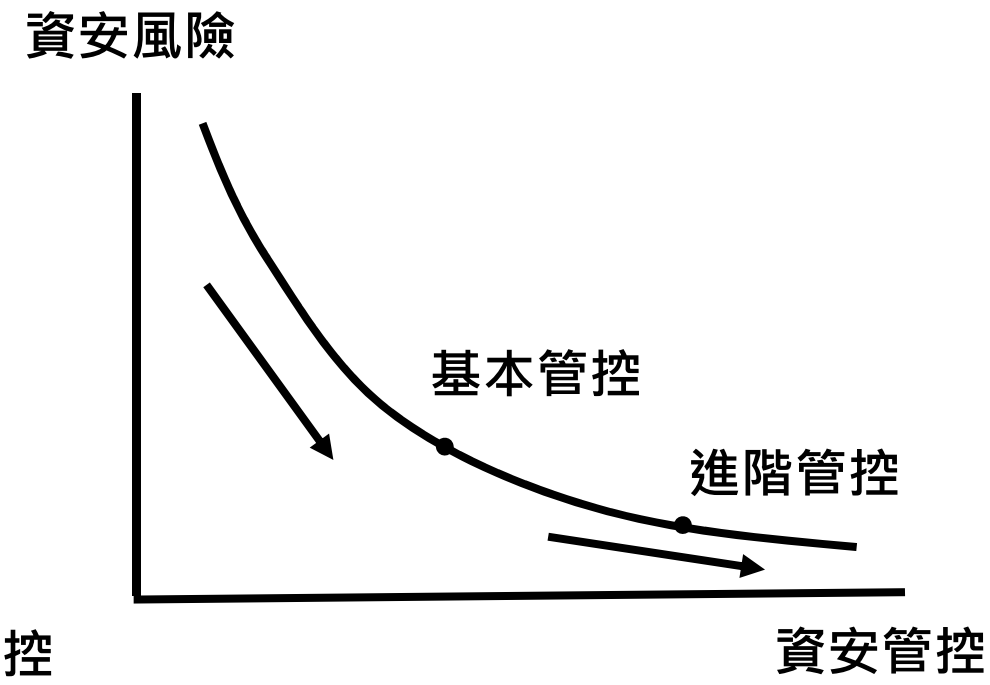
- 知錯能改
- 持續精進


PDCAサイクルを実行しよう
Plan (計画する)
Delay (遅れる)
Cancel (中止する)
Apologize (謝る)


PLAN
DO
ACT
CHECK

資安管控與成本考量






QUESTIONS
ANSWERS