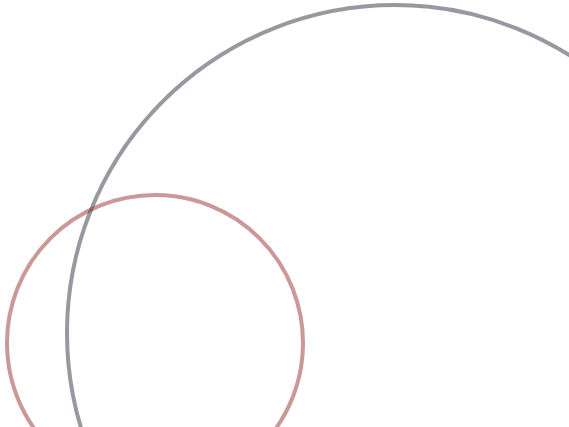
教育部國教署・115年度

校園資通安全專責人員知能研習

資通安全風險管理

亞洲大學　陳偉嵩



大綱

從盤點到風險改善

01　資通系統及資訊資產盤點　確認系統、業務、資產與防護需求。

02　風險評鑑作業　以高階或詳細方法辨識與評估風險。

03　風險改善作業　選擇處理方案，持續追蹤並再評鑑。

第一章

資通系統及資訊資產盤點

先看清楚服務、系統與資產，才能談風險。

盤點框架

資通系統盤點的四個焦點

系統分級作業

依安全等級評估方法判定防護需求。

核心與非核心業務

辨識持續運作不可中斷的服務。

資通系統防護基準

依等級落實對應資安要求。

RTO／RPO／MTPD

核心業務與分級邏輯

核心業務驅動之資通系統分級評估

依據「資通安全責任等級分級辦法」附表九，透過識別核心業務及其關鍵資通系統，判定防護需求等級（高、中、低），作為落實防護基準之起點。

1. 核心業務識別

確認機構之關鍵功能、法定職掌任務及關鍵基礎設施相關業務。

2. 資通系統關聯分析

盤點並識別支持上述核心業務持續運作之必要資通系統。

3. 防護需求分級評估

依機密性、完整性、可用性評估，定出高、中、低防護需求等級。

評估結論

分級結果直接決定該系統應符合之「資通系統防護基準」控制項目多寡與強度。

評估與控制流程

從業務影響評估到資安控制實施

1. 業務影響評估 (BIA)

針對核心業務進行 **服務持續性** 與 **CIA (機密性、完整性、可用性)** 評估，確認業務中斷對機關

2. 確定防護需求等級

依評估結果將系統劃分為 **高、中、低** 三種防護等級。等級越高，代表該業務對 CIA 的依賴

3. 選用安全控制措施

依據等級直接對應 附表 10 之控制要求，落實技術與管理面的防護基準，確保資源配置精準到位。

關鍵指標

CIA

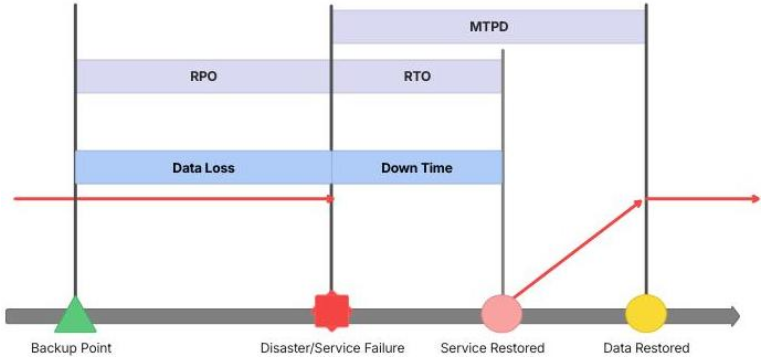
規範依據

表 10

防護目標

持續性

RTO／RPO／MTPD：三個關鍵問題



RPO｜資料遺失點

中斷後可接受的最大資料遺失量；決定了資料備份的頻繁程度。

RTO｜系統恢復時間

中斷後恢復業務運作的最大容許時間；決定了復原流程的速度。

MTPD｜最大中斷時限

業務可承受的最大中斷總時間；超過此限將導致不可挽回的損失。

共同目的

資訊資產

盤點作業是 ISMS 的基礎

管理制度的成效來自資通系統與資產的風險管理。應以資訊系統服務為主，確認各項服務涵蓋的資產內容。

- 以風險評估原則進行群組化
- 以 CIA 評估資訊資產重要性

資產類別與盤點核心

七類資產盤點，完整掌握服務依賴

人員

承辦、專案、開發、系統管理與計時作業人員。

硬體

伺服器、個人電腦、IoT 裝置與各類儲存媒體。

軟體

開發平台、管理平台、資安防護系統與資料庫。

資料

電子資料、日誌、影像、組態設定與原始碼。

文件

標準作業程序、合約、計畫書與系統架構圖。

環境

實體機房、辦公場域、電力供應與空調設施。

網路

區域網路、對外專線、路由器與資安閘道器。

盤點原則

依服務脈絡確認所有支援運作的關鍵資產。

第二章

資通安全風險管理

建立範圍、準則、角色與循環。

組織全景

風險管理從安全需求開始

依相關法規進行風險評鑑，確定資訊作業安全需求水準，採行適當且充足的資安措施，確保資訊蒐集、處理、傳送、儲存與流通安全。

01
識別需求

02
評估風險

03
採取措施

組織全景

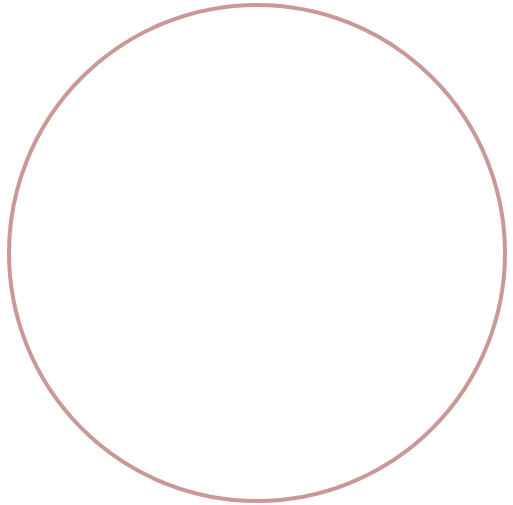
先界定內外部環境

外部環境

社會文化、政治、法律、科技、經濟、自然與競爭環境。

內部環境

治理、組織架構、角色責任、政策目標、能力、資源與知識。



管理準則

四項準則，讓判斷一致

風險管理作法

決定採用高階或詳細風險評鑑。

風險評估準則

建立資產、威脅、弱點與風險等級的判斷方式。

衝擊準則

定義機密性、完整性、可用性受破壞的嚴重性。

風險接受準則

決定哪些風險必須處理，哪些可暫時保留。

風險管理方法

兩階段方法：先快後深

Step 1｜高階風險分析

依附表九完成系統分級，再依附表十執行控制措施與風險處理。

Step 2｜詳細風險評鑑

對高安全等級系統，或資安事件後，進一步尋求適切處理方案。

風險評估

評估準則決定處理先後

風險評估準則的主要目的，是決定風險處理的優先順序，並支援風險處理計畫與控制措施的建立。

P
政策與程序

D
控制措施實作

C
監視與檢查

A
持續改善

資產價值

CIA：從三個面向衡量重要性

機密性 Confidentiality

資訊只能由適當對象接觸，避免機敏資料外洩。

完整性 Integrity

資料與系統維持正確、完整且未遭不當變更。

可用性 Availability

服務與資料在需要時可被使用。

取最大值

以 CIA 評估結果的最大值，定義資訊資產價值。

資產價值定義

不同資產，CIA 評估問題不同

資產類型	機密性 (C)	完整性 (I)	可用性 (A)
人員	接觸機敏資料程度	對其他人員的影響	異常時是否容易以他人取代
硬體	存放機敏資料程度	異常對其他設備影響	設備異常是否容易替代
軟體	處理機敏資料程度	異常時對資料的影響	軟體異常對整體服務的影響
文件	文件的機敏程度	文件錯誤影響程度	遺失文件對服務的影響
資料	資料之機敏程度	資料錯誤影響程度	資料提供使用範圍(服務)
環境	具備機敏資料程度	異常造成其他資產異常	異常影響的服務範圍
網路	具備機敏資料程度	異常造成其他資產異常	異常影響的服務範圍

威脅與弱點

威脅在外部，弱點在資產本身

威脅 Threat

來自資產外部，可能利用弱點造成影響。

弱點 Vulnerability

存在於資產本身，代表被利用的容易程度。

威脅與弱點評估

三級尺度，讓可能性可比較

等級	威脅發生可能性	弱點被利用容易程度
1	低：沒發生過或不可能發生	很難被利用
2	中：曾發生但次數很少	難易度適中
3	高：過去經常發生	很容易被利用

衝擊準則

衝擊，是威脅與弱點結合後的結果

衝擊準則定義機密性、完整性與可用性遭破壞時，對組織造成的嚴重性，可能包含營運受損、信譽損害、資安危害、業務與財務損失及違法情形。

普
輕微或可忽視

中
嚴重且影響業務

高
很嚴重、業務深遠受影響

衝擊範例

用 CIA 描述衝擊嚴重性

機密性「普」級

缺乏機密性保護，後果輕微或可忽視。

完整性「中」級

造成組織嚴重後果，且影響業務運作。

可用性「高」級

造成很嚴重後果，嚴重影響業務或導致信譽受損。

風險接受

有限資源下，先處理不能承受的風險

風險接受準則用來決定處理範圍。機關依任務性質、服務對象、資源與經費，排序風險並決定是否暫時保留。

優先處理

人員生命、法律與規範相關的衝擊，一律不得接受。

可能接受

普級且非生命／法律風險；中級可用性風險。

風險接受條件

三種情況可參考暫時接受

成本高於損失

風險處理成本高過潛在損失。

具備事件處理能力

風險發生後，機關有能力處理相關資安事件。

尚無有效技術

目前尚無有效的風險處理技術。

範疇與邊界

定義風險管理範疇時的考量

營運目標、策略及政策	施政業務維運過程
機關功能與結構	適用法令、法規及契約
資安政策	利害關係人期望
地理條件	社會文化環境
整體風險管理作法	資訊及資通系統資產

風險評鑑組織

跨部門，避免單一視角

建議成員

資訊、資安、總務、人事、會計及業務人員。

組成原則

納入最熟悉各部門業務與資產重要度的承辦人員。

避免偏誤

避免由單一成員執行全部評鑑，導致結果過於主觀。

組織分工

P／D／C／A 對應兩個小組

P｜規劃

規劃與推動小組掌管規範、審查與資安規劃。

D｜執行

執行小組盤點資產、辨識價值、風險與需求。

C｜確認

審核評鑑結果與風險處理計畫。

A｜改善

建置控制措施、撰寫計畫並實施改善。

組織角色

規劃推動小組：治理與審查

文件審核

審核資通安全維護計畫、實施情形、手冊、程序及指引。

成果審查

審查風險評鑑內容與風險處理計畫。

結果確認

審核風險評鑑結果與風險處理計畫。

組織角色

資安執行小組：評鑑與落實

盤點與分析

檢視資產與安控機制，鑑別價值、安全需求及實施狀況。

報告與建議

撰寫風險評鑑報告，建議修復等級並陳報。

計畫與控制

研議安控目標、撰寫風險處理計畫並實施措施。

第三章

風險評鑑作業

高階辨識、詳細分析，找到真正需要處理的風險。

高階風險評鑑

先保護最關鍵的系統

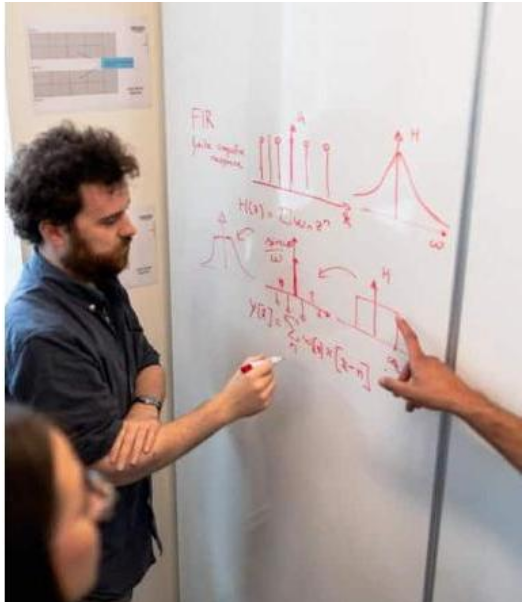
依系統分級結果進行快速風險評鑑，讓最關鍵且需受保護的系統優先被提出與實作。

把握時效

迅速因應風險。

有效運用資源

將預算投入關鍵系統。



高階評鑑範例

全球資訊網：一般性資訊服務

官方網站提供機關簡介與政策措施，未提供線上申辦服務。

機密性	普	皆為可公開的一般性資料
完整性	普	主要提供資訊公告
可用性	普	提供一般性資料瀏覽
法律遵循性	普	遵守智慧財產權及相關規定

詳細風險評鑑

八個步驟，從識別走到決策

1｜資產識別	2｜威脅與脆弱性識別
3｜現有控制措施識別	4｜後果識別
5｜後果評鑑	6｜事件可能性評鑑
7｜決定風險等級	8｜決定可接受等級

評鑑流程

風險識別 → 分析 → 評估

01

風險識別
資產、威脅、弱點、控制

02

風險分析
後果與事件可能性

03

風險評估
決定等級與接受範圍

第四章

風險改善作業

選擇適當方案，降低不利後果，並重新確認。

風險處理階段

處理不是終點，再評鑑才是閉環

依據評鑑結果

選擇適當風險處理方案。

衡量成本與利益

使風險不利後果合理降低。

完成後再評鑑

確認措施成效與剩餘風險。

風險處理方式

四種策略，對應不同情境

1　風險規避 Avoid

停止從事產生風險的活動。

2　風險降低 Reduce

降低發生機會或風險重大性。

3　風險移轉 Transfer

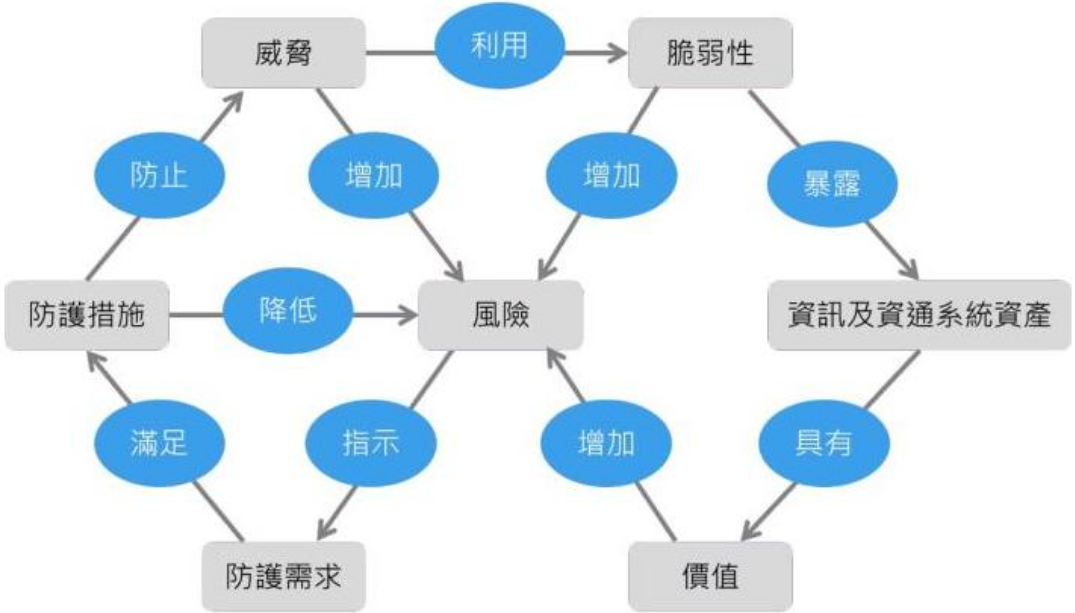
轉嫁風險與發生時的損失，例如購買保險。

4　風險接受 Retain

接受現狀，規劃承擔損失的方式。

風險管理關係

威脅、弱點、資產與控制彼此牽動



結語

看見資產，理解風險，持續改善

從盤點開始，以評鑑排序，透過適切處理守護校園服務。

謝謝聆聽