資安職能訓練-
資通系統風險管理
換證課程

行政院國家資通安全會報技術服務中心 編製

課程簡介

- 本課程的時間總長為3小時課程以「溫故知新」的原則，描述風險管理與危機處理作業知識，使學員於學習過程中，了解風險管理要素的內涵，熟悉評鑑作業技巧與風險處理原則

課程學習目標

- 本課程將帶領學習者溫習風險管理之架構與資安風險如何管理，並補充資通系統風險管理新知，進而學習鑑別、分析及評估資安的風險，讓學習者能夠養成資安風險處理能力，並有效控管各機關(構)可能之風險

- 知識(Knowledge)方面的學習目標
  - K1了解風險評鑑可以運用的方法
  - K2了解風險處理之重點與選用控制措施之原則
  - K3了解風險評鑑之變更管理
  - K4了解如何回饋風險評鑑知識

課程大綱

3 小 時	1.資通系統風險管理概論 2.風險管理流程與操作 3.風險評鑑案例分析

第1單元
資通系統風險管理概論

單元學習目標

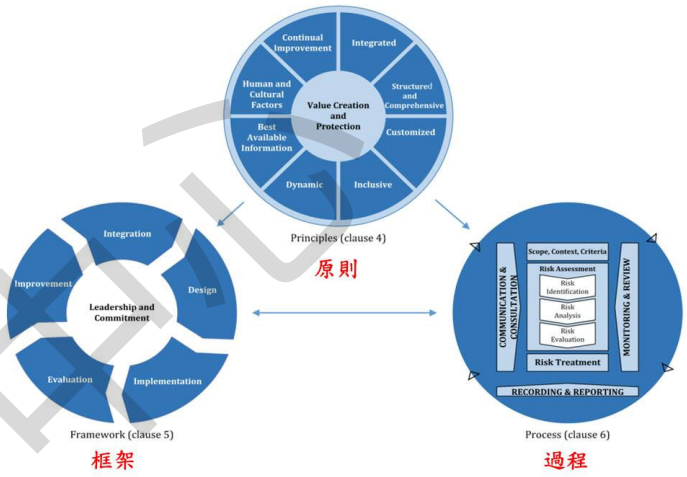
- 了解資訊安全管理的目的
- 了解CNS 27005風險管理過程之建立全景階段重點工作
- 以範例協助了解如何訂定風險管理準則
- 了解高階風險評鑑的作法與特色
- 了解詳細風險評鑑的作法與特色

風險管理原則、框架與過程關係

- 風險管理

  協同所有活動，以指導並控制組織所關注的風險

機關所有的活動均涵蓋在風險管理的範圍內，需對風險進行識別與分析，並評估風險處理方法的影響，滿足機關風險條件，以達成機關目標



資通系統風險管理換證課程 7

- 參考 CNS 31000 風險管理之原則、框架與過程

風險管理原則

- 風險管理的目的是創造與保護資產的價值，規範的原則為風險管理提供有效果且有效率的指導，傳達其價值並解釋其意圖與目的，風險管理原則如下：
  - 原則1：框架與過程應該客製化且互相對應
  - 原則2：利害關係人必須適當與及時的參與
  - 原則3：採用結構與全面的方法
  - 原則4：風險管理是組織所有活動的一部分
  - 原則5：風險管理應依預測、發現、告知及反應而執行變更
  - 原則6：風險管理應考慮可用資訊的限制
  - 原則7：風險管理的各個面向都會受到人文因素影響
  - 原則8：風險管理透過學習與經驗不斷改進
  - 前5項原則為設計風險管理措施提供指導，原則6、7及8則是與風險管理運作有關措施。

風險管理框架包含

- 領導與承諾
  - 將風險管理與組織的策略、目標及文化相結合。
  - 建立風險管理的方法、計畫或行動方案的聲明或政策。
  - 為管理風險提供必要的資源。
  - 確定可能或不可能採取的風險類型（風險偏好）。
- 整合
  - 確定管理當責、監管角色及職責。
  - 確保風險管理是組織所有功能的一部分，而不是與其分開。
- 設計
  - 了解組織及其內、外部背景。
  - 清楚說明風險管理承諾並分配適當資源。
  - 建立溝通與諮詢。
- 建置
  - 制定適當的實施計畫，包括最後期限等。

  - 定義由誰於何時、何處及如何進行不同類型的決策。
  - 在必要時修改適用的決策流程。
- 評估
  - 根據目的、建置及執行情形來衡量框架績效。
  - 確定風險管理框架是否仍適用於實現組織目標。
- 持續改善
  - 不斷監測與調整框架以解決外部與內部變化。
  - 採取措施以提高風險管理的價值。
  - 提高風險管理框架的適用性、充分性及有效性。

風險管理過程

- 風險管理過程以系統化將政策、程序及實踐，應用於溝通及諮詢、建立全景、風險評估、風險處理、風險監測與審查、風險記錄與報告等風險活動中

資通系統風險管理換證課程 10

- 溝通及諮詢
  - 於風險管理過程之各階段協同不同領域專家。
  - 協助從不同的觀點定義風險條件與評估。
  - 提供足夠的資訊來促進風險監督與決策。
  - 對受風險影響的人建立具包容性(inclusiveness)與歸屬感(ownership)的意識。
- 範圍、全景及準則
  - 界定風險管理活動的目的與範圍。
  - 界定組織的外部與內部環境。
  - 界定可接受風險與類型的風險準則。
  - 界定評估風險重要性與支持決策的準則。
- 風險評鑑
  - 風險鑑別主要在發現、識別及描述可能有助於或阻止目標實現及各種有形或無形的風險影響。
  - 對風險的類型與特徵進行風險分析，包括風險等級、風險來源、後果、可能性、事件、情境、控制及其有效性。

  - 風險評估係透過比較風險分析結果與使用的風險準則，確定風險的重大性以支持決策。
- 風險處理
  - 選擇最合適的風險處理方案。
  - 設計風險處理計畫，明訂如何實施處理選項。
- 監視與審查
  - 提高過程設計、實施及結果的質量與有效性。
  - 監視風險管理流程及其結果，監視與審查的責任須清楚界定。
  - 計畫、收集及分析所得資訊、記錄其結果，並提供回饋。
  - 將結果納入績效管理、衡量及報告活動。
- 記錄與報告
  - 在整個組織內溝通風險管理活動與結果。
  - 為決策提供資訊。
  - 改進風險管理活動。
  - 提供風險資訊並與利害相關者進行互動。

政府機關風險管理架構(1/2)

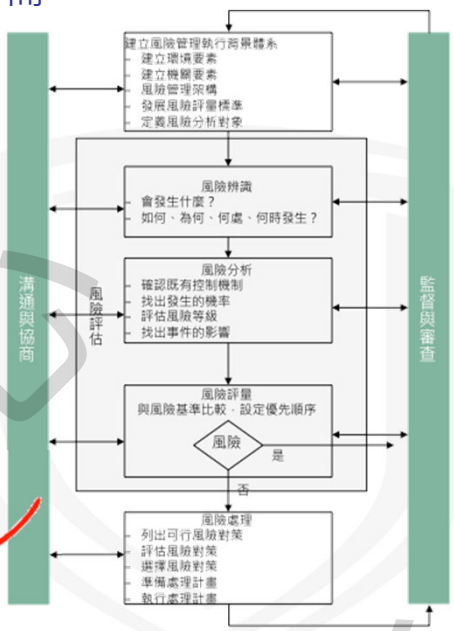
- 行政院所屬各機關風險管理及危機處理作業基準
  - 於97年12月8日行政院所修正並發布
  - 為推動各部會將風險管理及危機處理融入日常作業與決策運作，以降低災害之可能及後果，達成施政目標、提升機關績效
  - 本基準係原則性之作業規範，做為協助各部會推動整合性風險管理及危機處理之參考依循，並藉由風險管理及危機處理作業手冊，引導各部會建立標準作業程序並進行實務性操作
  - 各部會得依相關法令及業務特殊需求管理其風險或危機

- 為改善機關治理、降低財務損失、提升運作效益、達成施政目標，及掌握創新突破機會，以防範及消減施政風險之衝擊，並促使各部會將風險管理融入日常作業及決策運作
- 97年4月1日函頒「行政院所屬各機關風險管理作業基準」，而97年12月8日行政院為進一步強化機關危機處理能量，爰將前開基準納入「危機處理」專章，並配合將名稱修正為「行政院所屬各機關風險管理及危機處理作業基準」，機關各層級參酌作業基準運作時，須設定政策目標、規劃及建置架構、執行與操作、監督審查與矯正預防及改善等作業

政府機關風險管理架構(2/2)

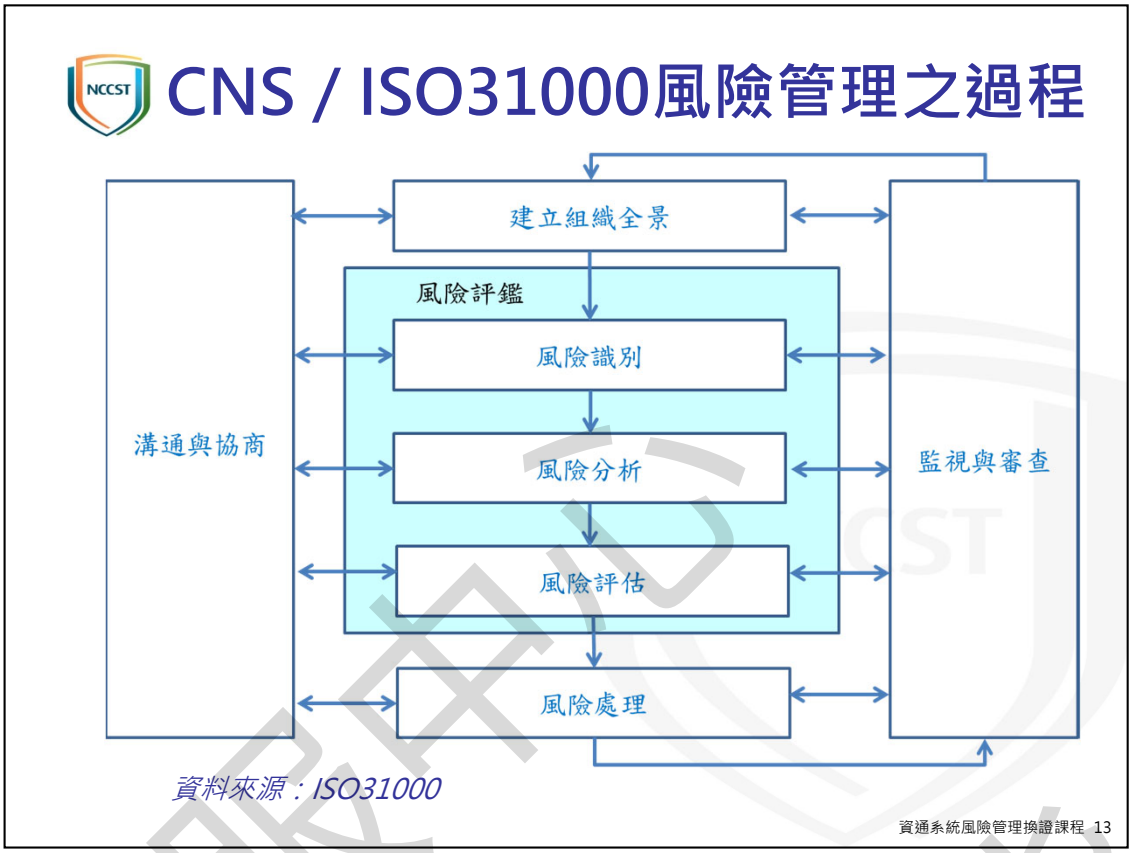
- 風險管理及危機處理作業手冊

風險管理及危機處理作業手冊，強調風險管理是一個「持續改善」的反覆過程或循環過程，以協助政府部門改善績效並達成公共價值(Public Value)，另可促成行政部門提供更好的服務、資源的更有效使用、更佳的計畫管理、避免貪瀆與浪費公帑並鼓勵創新



參考CNS 31000之風險管理過程所擬定

- 風險管理及危機處理作業手冊，參考CNS 31000 風險管理過程



- 風險管理的過程應符合下列事項之要求：
- 是機關整體管理活動中，不可或缺的一部分。
- 應融入於機關文化之中。
- 應根據機關的活動過程加以調適。

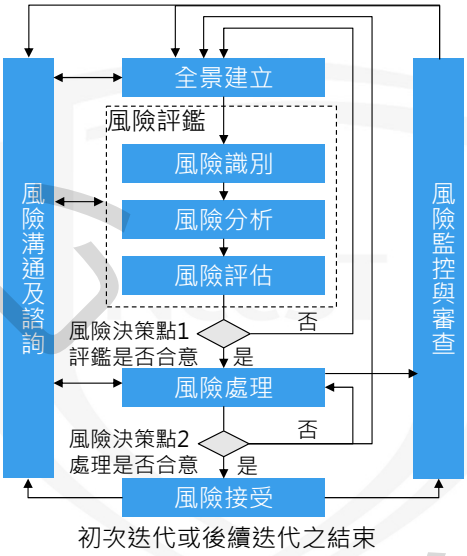
CNS27005資訊系統風險評鑑

- CNS 27005不提供任何資安風險管理之特定方法論
- 組織可自行依據，例如：資安管理系統(ISMS)範圍、風險管理全景或產業別等，定義風險管理作法
- 有數種方法論，能在CNS 27005描述框架下，實作資安管理系統(ISMS)之要求

☑ 遵循CNS 31000之規定，以循環作法(亦稱為迭代式)進行風險評鑑

☑ 循環作法提供在最小化花費，於識別控制措施之時間與耗費間良好平衡時，以確保高風險被適當評鑑

CNS 27005資安風險管理過程，遵照CNS 31000規定，並與行政院風險管理與危機處理作業手冊中，陳述的管理架構一致，均符合國際風險管理規範要求



- CNS 27005提供資安風險管理的指導綱要，並支援 CNS 27001資訊安全管理系統 (Information Security Management System, ISMS)的特定要求
- 參考CNS 27005風險管理過程
  - 首先建立全景，然後進行風險評鑑
  - 若能提供充分資訊，有效地修正風險，至可接受等級所需措施，則評鑑工作完成，隨後展開風險處理
  - 若資訊不充分，則需進行再一次的修訂全景(例如：風險評估準則、風險接受準則或衝擊準則)之風險評鑑循環
  - 此循環可能僅及於整體範圍之有限部分「風險決策點 1」
  - 風險處理有效性，依風險評鑑結果而定，可能無法立即將剩餘風險降至可接受等級，若有需要，可變更全景參數(例如：風險評鑑、風險接受或衝擊準則)後，進行另一次風險評鑑循環，再執行更進一步風險處理「風險決策點 2」

建立全景(Context Establishment)

- 目的
  - 了解機關對資安管理的期望與需求，宜由機關高階長官(例如資訊安全長)明訂，包括：
    - 資安政策，明確界定出風險評鑑範圍、角色及責任等
    - 識別該機關內與外各方面的安全需求
- 建立全景三項重點工作
  - 規劃與定義風險管理基本準則
  - 確認資通系統範疇與邊界
  - 成立「跨部門」的風險評鑑組織

- 建立全景的目標在於了解機關對資安管理的期望與需求，宜由機關高階長官(例如：資訊安全長)明訂。政府機關應該在其機關資安政策中，明確聲明該機關施政業務相關資通系統應執行風險評鑑，並界定出風險評鑑範圍、角色及責任等。
- 建立全景應注意要識別機關內、外各方面的安全需求，包括機關的資訊安全政策、法令、法規、規章及合約。其次要規劃與定義「風險評估準則」、「衝擊準則」及「風險接受準則」等風險管理基本準則。接著界定風險評鑑範圍，並清查盤點該範圍內所有相關的資通系統。若選用「詳細風險評鑑作法」，則需清查盤點該資通系統的所有資訊資產，同時整合這些資通系統與資訊資產可能涉及的跨部門業務成員，共同組成資通系統風險評鑑組織，有助於執行與落實風險評鑑的成效。

- ISO/IEC27005並不提供任何資安風險管理之特定方法論。組織可自行依據例如資安管理系統(ISMS)之範圍、風險管理之全景或產業別等，定義其風險管理作法。有數種現存方法論，能在本標準描述之框架下，以實作資安管理系統(ISMS)之要求。
- 風險管理過程的高階觀點，遵循ISO 31000之規定，資安風險管理過程之風險評鑑及/或風險處理活動，以循環作法(亦稱為迭代式)進行風險評鑑能在每一循環中增加評鑑之深度與詳細度。循環作法提供在最小化花費於識別控制措施之時間與耗費間之良好平衡時，以確保高風險被適當評鑑 。

衝擊準則(Impact Criteria)

- 衝擊準則(Impact Criteria)主要訂定當威脅與脆弱性結合，破壞資訊及資通系統資產的機密性、完整性及可用性(CIA)，對組織衝擊的嚴重性，可能包括營運受損、信譽損害、資安危害、業務與財務價值損失及違法情事等
- 建議將衝擊嚴重性，以機密性、完整性及可用性遭破壞的程度，分為普、中、高3等級，分別說明各等級對組織的影響，例如
  - 機密性「普」級：資訊缺乏機密性保護，造成後果輕微或可忽視
  - 完整性「中」級：缺乏完整性保護，會造成組織嚴重後果，且災害會影響組織業務運作
  - 可用性「高」級：缺乏可用性保護，造成後果很嚴重，且災害會嚴重影響業務或信譽受損

- 當威脅與脆弱性結合，將破壞資訊資產的「機密性」、「完整性」及「可用性」，應根據衝擊準則評估其對組織衝擊的嚴重性。衝擊可能包括營運的受損、信譽的損害、資訊安全的危害、業務與財務價值的損失及違法情事等，建議將衝擊的嚴重性以「機密性」、「完整性」及「可用性」遭破壞的程度分為三個等級(普、中、高)。例如：「機密性」的「普」級：公開資訊缺乏機密性保護，所造成後果輕微或可忽視者。
- 衝擊可能包括營運的受損、信譽的損害、資訊安全的危害、業務與財務價值的損失及違法情事等，如何訂定衝擊的準則？舉例來說：
- 可以根據影響的範圍，例如：影響全機關、影響各處室、影響個人或影響輕微。
- 可以根據財務損失的狀況，例如：損失千萬以上、損失百萬～千萬或損失百萬以內。
- 可以根據信譽損害的程度，例如上國際新聞媒體、上全國性新聞媒體或上區域性新聞媒體。
- 可以根據可用性喪失的程度，例如：中斷1天以上、中斷8hr以上或中斷4hr以上。

風險接受準則 (Risk Acceptance Criteria)

- 【風險接受準則】可依預期風險存在時間長短而不同，例如：風險可能與一暫時或短期的活動有關。設定風險接受準則，宜考量下列項目：
  - –業務需求目標
  - –法律、法令、規章及合約方面的要求
  - –智慧財產權(Intellectual Property Right， IPR)
  - –資源分配狀況
  - –技術成熟度
  - –經費預算
  - –社會與人道主義因素

- 機關會因其所負責業務之類別與性質、服務對象、內部資源及經費預算等因素，影響其風險接受準則的訂定。
- 風險接受準則得用以具體指定風險處理的範圍與標的，包括有：
  - 無法接受違反個資法情事；
  - 接受系統或業斷中斷4hr以內；
  - 關鍵業務不得中斷超過1hr；
  - 無法接受全面侵害智慧財產權情事，對同仁自行下載導致侵權行為，透過教育訓練加強輔導；
  - 接受現有資訊技術無法克服的風險，但須有處理方式，且處理方式不得超過最大容許中斷時間。

舉例來說，無法接受違反個資法情事，所以會造成個資外洩的高風險資產就應納入風險處理的範圍。又比如說，接受系統或業務中斷4hr以內，所以會中斷超過4小時的資產就應該納入風險處理的範圍。

高階風險評鑑

- 作法
  - –對資通系統先做概略風險分析
  - –對高風險之資通系統，再進行詳細的風險分析
  - –其他一般資通系統，則利用高階風險評鑑，選擇相對應基本控制措施
- 特色
  - –投入時間與資源前，先進行高階風險分析，得到廣被接受的風險分析計畫
  - – 能迅速地建立一個組織安全計畫的策略構圖
  - – 優先對最需要受到保護的系統施以防護措施
  - –若評估不正確，將影響控制措施的選擇

- 高階風險評鑑乃是組織基於各種人力、預算、時間或資源等理由或限制，首先針對其內部所有資通系統與資訊資產，進行初步的「高階風險評鑑」，找出每個資通系統在該組織的營運業務價值，從「高階衝擊影響」開始，而不用從資產價值、威脅、脆弱性及後果等系統化的詳細風險評鑑開始。
- 被識別為「重要」及/或「高風險/高衝擊影響」的資通系統，組織可運用「詳細風險評鑑作法」對其進行「下一個」風險評鑑循環。屬於「較不重要」或「較低風險/較低衝擊影響」的資通系統，組織則可自行根據其安全要求與風險評鑑目標「自行選擇」適用的風險評鑑方法進行風險處理。
- 高階風險評鑑的特色：能迅速因應，把握時效；該組織最關鍵且需受到保護的資通系統將會被優先提出與實作；且資源預算可以獲得有效運用。
- 要特別注意的是：如果初期的「高階風險評鑑」不精確，某些資通系統可能被識別為不需要進行詳細風險評鑑，將影響控制措施的選擇。

詳細風險評鑑

- 作法
  - –對資通系統的所有資產做風險評鑑
  - –深入的識別資產與估價、威脅對資產的評鑑及脆弱性的評鑑
  - – 分析風險所造成的衝擊與其可能性
  - – 識別出目前的安全防護措施
- 特色
  - –較可鑑別出所有資產的風險，實施適當的保護措施
  - –分析所得結果可被用在風險評鑑的變更管理
  - –比較耗費人力

詳細風險評鑑的作法：

- 首先對機關內所有資通系統的資訊資產，逐一詳細清查風險。接著深入的識別「資產」與其價值、「威脅」對資產的評鑑及「脆弱性」的評鑑，據以分析風險所造成的「CIA 衝擊」與其「可能性」。
- 詳細風險評鑑的特色：
  - 所有資訊資產均能識別出該資產的風險，並對該資訊資產作適當的防護控制措施。
  - 針對資訊資產所作詳細風險評鑑之結果，未來可被運用在該組織或該資通系統變更管理時安控機制之參考。
  - 應特別注意的是：
  - 因針對資產進行較為詳細的風險評鑑，資料龐大難以維護。且會耗費大量專業人力、時間及與預算資源。因此適用於「特定、關鍵」的資通系統。

第2單元
風險管理流程與操作

單元學習目標

- 了解如何實作高階風險評鑑作法
- 了解如何實作詳細風險評鑑作法
- 了解風險處理與建立全景的關係
- 了解4種風險處理策略的定義與差別
- 了解控制措施選擇原則，以利日後選擇最適合機關的控制措施進行實作
- 了解控制措施選擇主要來源

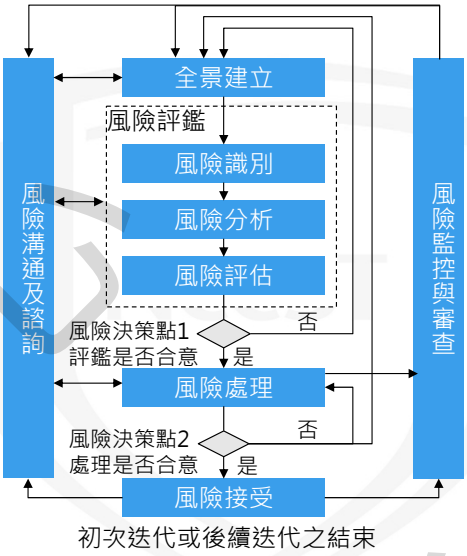
CNS27005資訊系統風險評鑑

- CNS 27005不提供任何資安風險管理之特定方法論
- 組織可自行依據，例如：資安管理系統(ISMS)範圍、風險管理全景或產業別等，定義風險管理作法
- 有數種方法論，能在CNS 27005描述框架下，實作資安管理系統(ISMS)之要求

☑ 遵循CNS 31000之規定，以循環作法(亦稱為迭代式)進行風險評鑑

☑ 循環作法提供在最小化花費，於識別控制措施之時間與耗費間良好平衡時，以確保高風險被適當評鑑

CNS 27005資安風險管理過程，遵照CNS 31000規定，並與行政院風險管理與危機處理作業手冊中，陳述的管理架構一致，均符合國際風險管理規範要求



- CNS 27005提供資安風險管理的指導綱要，並支援 CNS 27001資訊安全管理系統 (Information Security Management System, ISMS)的特定要求
- 參考CNS 27005風險管理過程
  - 首先建立全景，然後進行風險評鑑
  - 若能提供充分資訊，有效地修正風險，至可接受等級所需措施，則評鑑工作完成，隨後展開風險處理
  - 若資訊不充分，則需進行再一次的修訂全景(例如：風險評估準則、風險接受準則或衝擊準則)之風險評鑑循環
  - 此循環可能僅及於整體範圍之有限部分「風險決策點 1」
  - 風險處理有效性，依風險評鑑結果而定，可能無法立即將剩餘風險降至可接受等級，若有需要，可變更全景參數(例如：風險評鑑、風險接受或衝擊準則)後，進行另一次風險評鑑循環，再執行更進一步風險處理「風險決策點 2」

高階風險評鑑

高階風險評鑑簡介

- 根據ISO/IEC 27005
- 對內部所有資通系統，找出營運價值與高階衝擊影響
- 不須對所有資通系統的所有資訊資產，以資產價值、威脅、脆弱性及後果的系統化詳細風險評鑑開始
- 基於人力、預算及時間考量來運用

- 高階風險評鑑的特色：
  - 機關可迅速鑑別出內部所有資通系統的安全等級或關鍵程度，有助於先對較關鍵或衝擊影響較大的系統做基本的防護。
  - 高階風險評鑑是以資通系統整體考量為主，評鑑其機密性，完整性及可用性喪失所造成的影響。並未細到各項資產。
  - 機關宜考量人力與預算，先對機關的資通系統執行高階風險評鑑，有助於將有限的預算投入較關鍵系統的保護。
  - 高階風險評鑑主要是針對資通系統來作評鑑，而詳細風險評鑑則會細到每一項資產，可見得詳細風險評鑑是較耗費人力的一項工作。

- 高階風險評鑑只針對機關的資通系統來作評鑑，依四大構面分別評鑑出高、中或普。可讓機關高階長官在最短時間內了解機關內所有資通系統的安全等級究竟為高、中或普，並決定將人力或預算先投入在保護安全等級高的資通系統。
- 但高階風險評鑑畢竟只針對資通系統做較初步的評估，考量得不夠嚴謹，若評鑑有誤，可能導致投入過多的預算在保護安全等級誤評為高的系統；當然也有可能是將安全等級高的系統誤評為中，僅對此系統實施安全等級中的安控措施，而未實施安全等級高的安控措施，導致安控措施不足的情形。

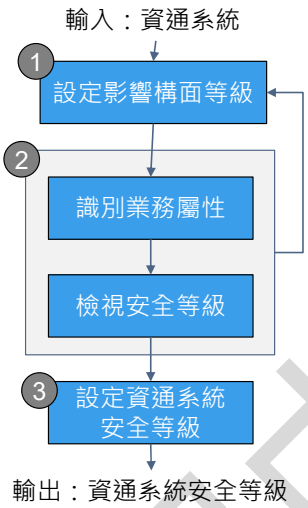
- 進行高階風險評鑑的前置作業：
  1.應先了解機關本身特性與目標，並進行營運衝擊分析等，以辨識核心業務，也就是要先了解機關高階長官心目中認定哪些系統是重要的，例如：最大容許中斷時間十分短。
  2.應視機關本身業務特質，先行研訂符合機關業務需求之影響構面與安全等級分級準則。
  機關應依資通系統分級與資安防護基準作業規定所提的四大構面評估，建立適合機關評鑑及安全等級。
  3.實務上，機關可視需要在實施資通系統分類分級前，先進行資通系統盤點，盤點出機關負責的系統究竟有多少後，才能確保所有的系統都已評鑑，沒有疏漏。
- 等上述3項前置作業都準備妥當後，才適合進入高階風險評鑑，評估安全等級。

高階風險評鑑作法

- 直接依資通系統分級結果，做風險評鑑
- 採用下列2種方式
  - 企業衝擊分析
  - 資通安全責任等級分級辦法
- 特色與注意事項
  - 把握時效，迅速因應，讓最關鍵且需受保護的資通系統，優先被提出與實作
  - 資源預算有效運用
  - 初期高階風險評鑑不精確，資通系統將可能被識別為不需再執行詳細風險評鑑

高階風險評鑑作法

依「資通安全責任等級分級辦法」執行



資通系統分級處理程序

1. 由業務承辦人依機密性、完整性、可用性及法律遵循性4大影響構面，分別評估對各資通系統影響衝擊，並據以設定影響構面等級
2. 識別資通系統所支援之業務屬性，並由承辦單位主管檢視業務承辦人所設定安全等級之合理性
3. 資通系統安全等級，經承辦單位主管與資訊主管確認後，最後由資訊安全長核定

- 行政院國家資通安全會報，要求機關依據「資通安全責任等級分級辦法」，評鑑資通系統安全等級，為高階風險評鑑的最佳實務作法
- 高階風險評鑑過程，分為3個步驟

高階風險評鑑作法

- 依「資通安全責任等級分級辦法」的安全等級評估方法，以「全球資訊網」為範例
- 全球資訊網：官方網站，提供機關簡介與介紹政策措施，無提供線上申辦服務

資通系統安全等級，取其4大影響構面安全等級最高者

影響構面		安全等級	原因說明
1.機密性	初估	普	網站資訊皆為可公開的一般性資料
	異動		
2.完整性	初估	普	主要提供資訊公告
	異動		
3.可用性	初估	普	提供一般性資料瀏覽
	異動		
4.法律遵循性	初估	普	必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及相關規定，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果
	異動		

業務屬性

- 行政類
  - 指機關內部輔助單位之業務（如：人事、薪資等）若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其類別。
- 業務類
  - 在政府營運持續的概念下，政府機關在遭遇衝擊時，須確保能持續運作之關鍵業務與民眾重要生活機能息息相關之關鍵基礎建設。

- 業務屬性大致分為兩類：(原區分為行政性、關鍵性及支援性三大類，104年7月版已刪除支援性業務，改為行政類及業務類兩類)
- 行政類業務：指機關內部輔助單位之業務（如：人事、薪資等），惟若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其類別。
- 業務類業務：指機關內部業務單位之業務（如：交通監理、便民服務等）。

資通系統安全等級分級範圍

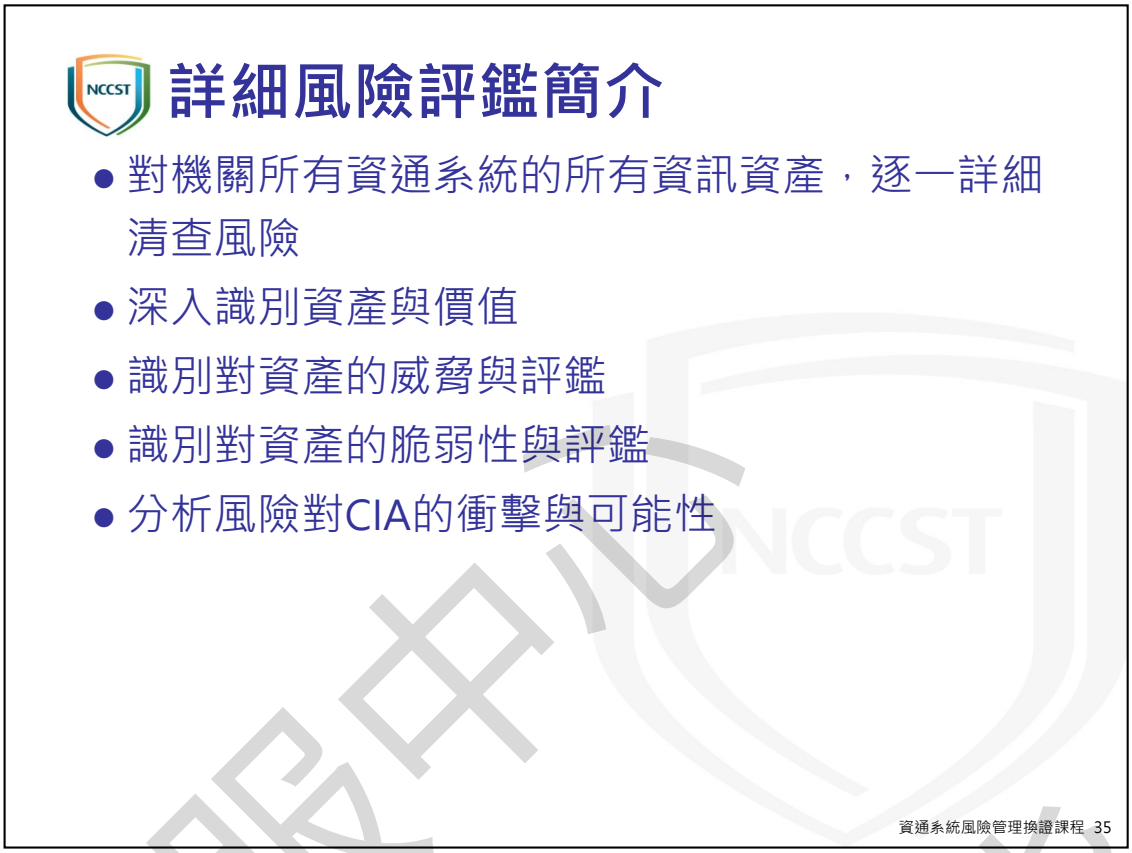
- 需要進行分級之資通系統，以自行或委外開發之資通系統為主。
- 由上級或其他機關開發之共同性系統之分級，統一由開發管理之機關進行評估與鑑別，如電子公文交換系統，不需納入資通系統分級範圍。
- 套裝軟體、作業系統或防毒系統、防火牆系統、入侵偵測/防禦系統、弱點掃瞄系統、網頁/郵件內容過濾系統等屬資安防護處理相關控制措施，均不需進行資通系統分級。

資通系統安全等級設定原則

- 衡量系統於機密性、完整性、可用性及法律遵循性等4大構面喪失時可能造成的衝擊，據以評估設定安全等級
- 安全等級範例
  - 普(等級1)、中(等級2)及高(等級3)
  - A(高) 、B(中) 、C(普通) 及D(低)
- 安全等級愈高表示對資安防護需求水準要求愈高
- 資通系統之安全等級，取其四大影響構面安全等級最高者。

- 安全等級分為【普】、【中】、【高】三級，由機關依機密性、完整性、可用性及法律遵循性四大影響構面，分別考量資通系統於發生資安事件時可能造成之衝擊，即衡量資通系統資料外洩、資料遭竄改、系統故障等情事時可能造成的後果嚴重程度，並據以評估、設定安全等級。
- 資通系統於發生資安事件時，通常會同時衝擊多個影響構面。當資通系統發生資料外洩時，可能衝擊「機密性」、「完整性」、「法律遵循性」等影響構面；當資通系統發生資料遭竄改情形時，可能衝擊「機密性」、「完整性」、「法律遵循性」影響構面；而當資通系統發生系統故障情形時，則可能衝擊「可用性」、「法律遵循性」等影響構面。此外，若系統發生資安事件時，對於某個影響構面不造成任何危害，則該影響構面安全等級以NA 表示不適用。資通系統之安全等級，取其四大影響構面安全等級最高者。

詳細風險評鑑



- 對機關所有資通系統的所有資訊資產，逐一詳細清查各項資產風險。例如：辦公室自動化OA系統是指辦公室自動化主機設備、辦公室自動化主機OS、辦公室自動化系統防毒軟體、辦公室自動化應用系統、辦公室自動化系統資料庫、辦公室自動化系統程式碼、辦公室自動化系統備份工具、辦公室自動化系統開發工具、辦公室自動化系統運作相關網路設備、辦公室自動化系統管理者、辦公室自動化系統維護廠商及辦公室自動化系統使用者等，詳細風險評鑑針對辦公室自動化系統，就要針對上述的資產逐一評鑑其風險。
- 而其步驟會詳細到需要深入識別資產與價值，此價值即是對辦公室自動化系統主機...辦公室自動化系統使用者等資產，逐一評鑑其發生機密性，完整性及可用性喪失時，所造成的衝擊影響程度。
- 接著識別對資產的威脅並評鑑其威脅發生的機率與識別資產的脆弱性被利用的難易度，以分析風險對資產的CIA喪失的衝擊與可能性。

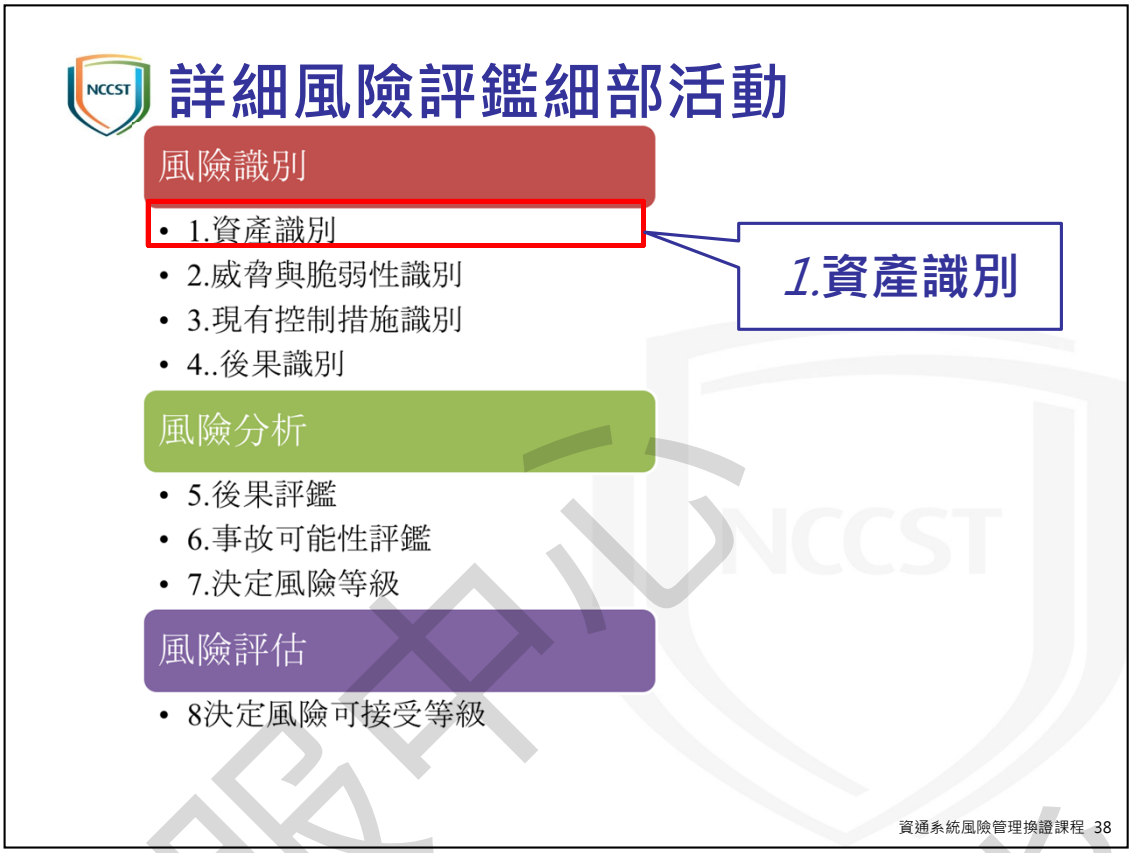
詳細風險評鑑的特色與注意事項：

- 因為詳細風險評鑑是針對資產做評鑑，可分別對不同資產施以不同安全等級(高、中、普)的安控措施，因此能辨別出最適當的防護措施。
- 由於會仔細評鑑到各項資產，若有任何風險變更(例如：移轉系統或更換廠商)，可以僅針對會受到影響的資產做不同程度的異動管理。
- 資通系統的定義為協助組織決策、協調、控制、分析及實行，負責蒐集、處理、傳送、儲存及流通資訊的一組資產，所以詳細風險評鑑會針對資通系統的資產做評鑑，較耗費人力與時間，因此，也需要對詳細風險評鑑作法較了解的專業人員協助處理，才能有效地評鑑。
- 因針對資產進行較為詳細的風險評鑑，資料龐大，造成維護上的困難。

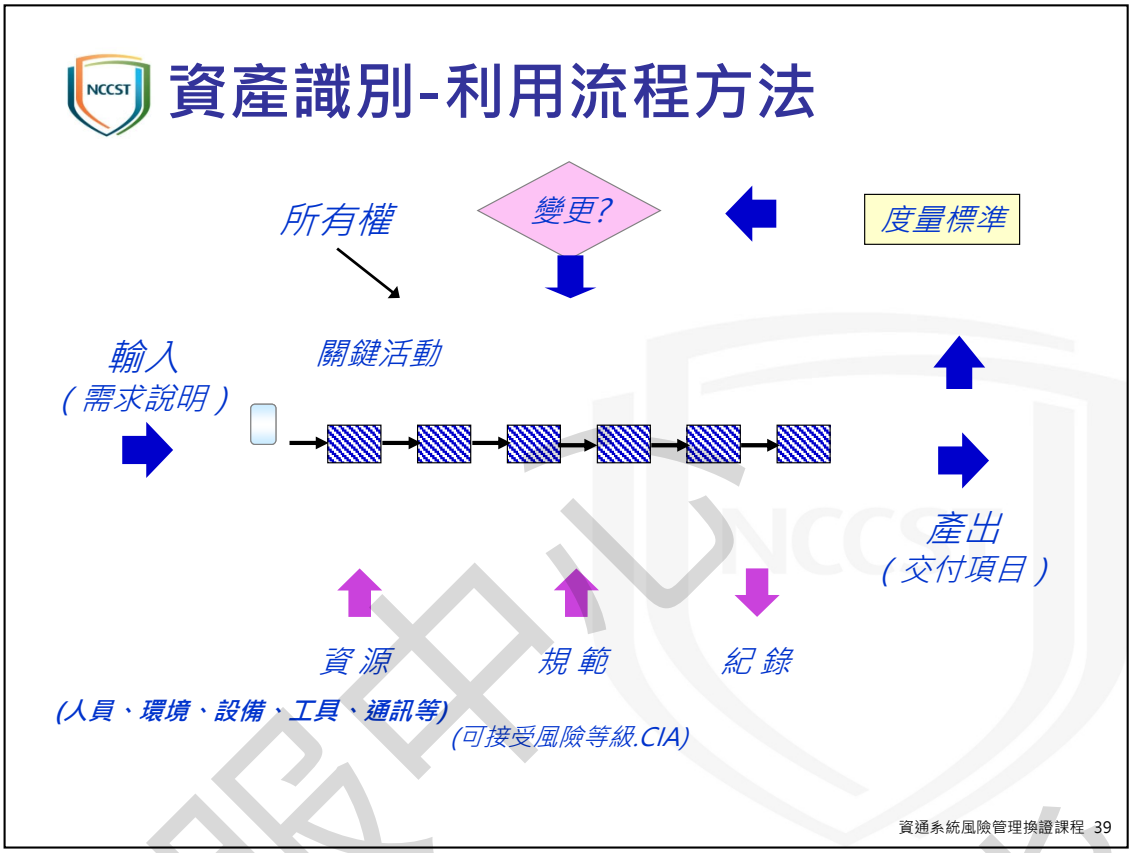
詳細風險評鑑細部活動程序

- 風險識別
  - 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
- 風險分析
  - 5.後果評鑑
  - 6.事故可能性評鑑
  - 7.決定風險等級
- 風險評估
  - 8決定風險可接受等級

- 此細部活動程序圖出自於資通系統風險評鑑參考指引，其主軸是依照ISO27005的敘述，再考量實際執行時搭配工具的可行性與方便性，微調步驟而成。
- 主架構仍維持風險分析與風險評估，而風險分析又分為風險識別與風險估計，這部分未改變。
- 8個步驟將在後續一一詳細說明。



- 現在說明詳細風險評鑑的第1個步驟資產識別



將流程方法以流程圖的方式呈現。

- 度量標準指的是評估採購作業的績效指標，例如：採購作業超過預期3天完成的件數超過xx件，透過訂定一些指標量測採購作業的績效與有效性。
- 透過度量標準，調整不適切的作業模式，藉此改善整個流程。
- 透過流程方法分析整個作業流程，例如：機房維運作業流程，因機房維運涵蓋面廣，包括主機設備維護作業、門禁維運作業、消防系統維護作業、攝影系統維護作業、UPS、環控...等。
- 例如：採購作業流程通常是由業務單位提出需求，這個獲得需求單位主管同意的採購需求就是採購作業流程的輸入，未授權同意的需求不能算是輸入，因為根本無法進入採購流程。負責採購業務的承辦同仁就是所有權。簽訂契約通常代表採購作業的完成，所以契約可說是採購作業的輸出。
- 關鍵活動可能是：

  1.若屬資訊設備將會簽資訊部門，取得資訊單位同意。

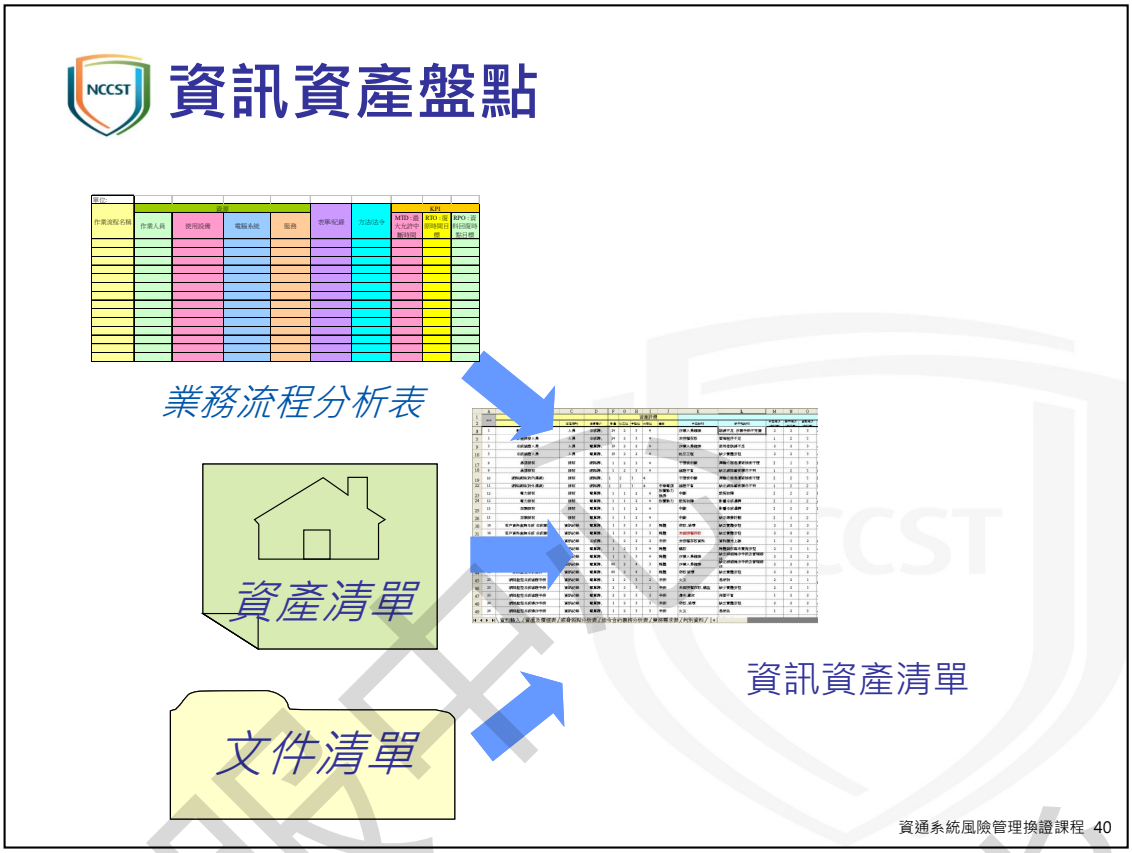
  2.將RFP等相關資料公開招標。

  3.依投標廠商評選或以價格標決定廠商。

  4.通知廠商評選與議價。

  5.通知得標廠商交付履約保證金。

  6.與廠商簽訂契約。
- 流程中會使用到的資源可能是承辦業務與經辦的相關人員，可能會使用採購系統，可能會有採購系統的主機。
- 而標準/規範就是指採購法(採購作業要依採購法進行，一般民間企業可能依內部訂定的採購程序辦法來執行，這就是規範)。
- 紀錄就是指採購過程中留下的紀錄，例如：公開上網招標的相關資料、廠商投標聲明書、廠商投標的建議書及廠商簡報資料等，這些都屬於資產。



- 透過工具盤點與彙整資產是一個常用的好方法，使用Excel表建立資產清冊最為便利。
  1. 透過流程方法記錄下輸入、輸出及關鍵活動所使用的資源、規範或法律，在左邊的第一張表內。
  2. 機關既有的資產清單也是一個好的參考依據(包含設備與採購的合法軟體都是資產)。
  3. 機關既有的文件清單也是一個好的參考依據(文件也都是資產)。
- 將上述3項表格彙總起來就是資訊資產清單初稿。

- 再利用深度防禦模型Double Check，以確認所列資產的完整性。
- 由於標準要求要列出資產的保管人/負責人，這點很重要。
- 以公文系統為例說明如何提列資產：
  1. 公文設備主機與公文設備主機的作業系統，通常由機房主機管理者提列(因主機管理者是Owner)。
  2. 公文系統由開發團隊提列，一般機關並未將權責切割得非常細，建議資料紀錄亦應由開發團隊同仁提列較適切。
  3. 公文系統假設是架在MS SQL資料庫，則MS SQL應該由DBA提列。
  4. 公文系統使用的網路設備應由資訊部門網路管理者提列。
  5. 使用者在此泛指所有會使用到的人員，應包含委外廠商，委外廠商分2種，設備維護廠商應由資訊部門提列，委外開發廠商應由開發團隊提列。
- 光是一個公文系統就包括這麼多資產，又由不同的Owner提列，這也是非常好的一種Double Check機制。
- 例如：開發團隊提列出他們所有的系統，查核這些系統的主機是否都提列了，就知道有沒有漏列設備，彼此交錯查核。

- 現在說明詳細風險評鑑的第2個步驟威脅與脆弱性識別

威脅種類

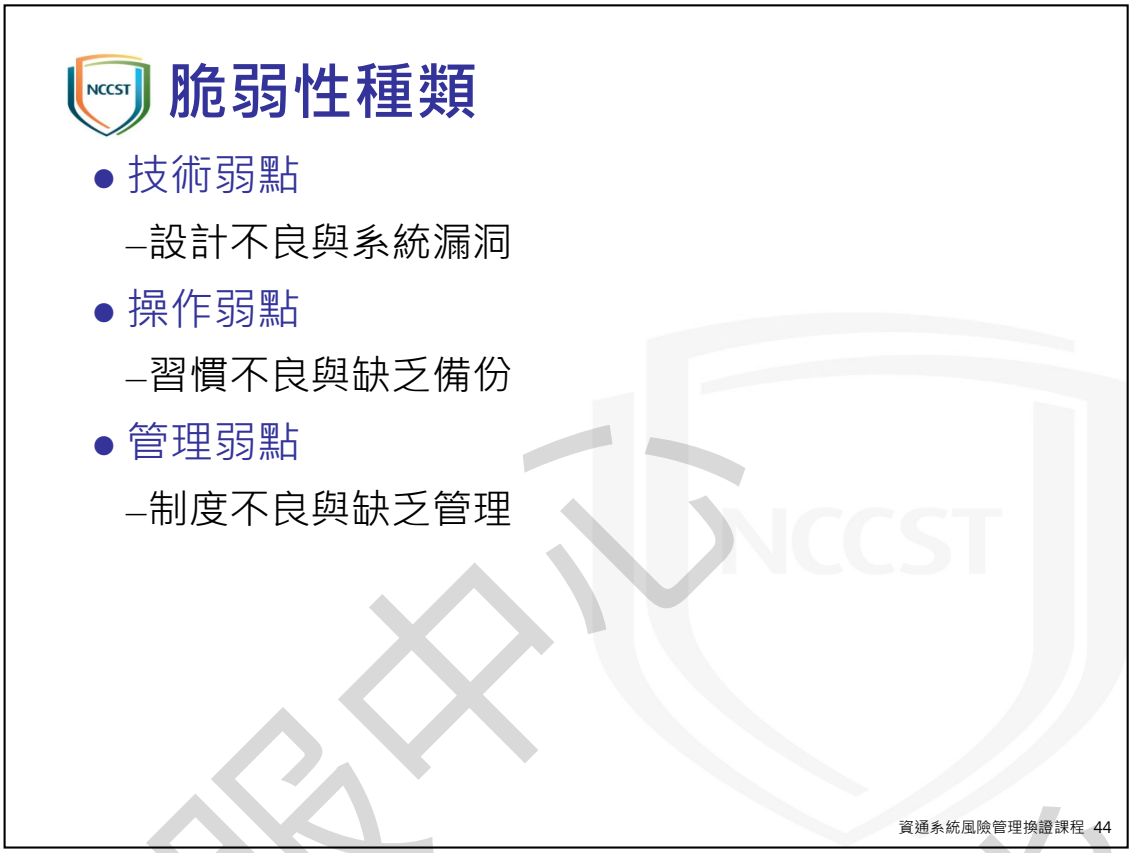
- 天然威脅
  - 水災、地震、颱風及土石流
- 環境威脅
  - 火災、長期停電、污染及治安

- 人為威脅
  - 無意的行為：打錯資料、誤刪檔案及踢到插頭
  - 有意的行為：竊盜、惡意破壞及放置後門

- 系統威脅
  - 硬碟壞軌、當機及網路中斷

資通系統風險管理換證課程 43

- 威脅種類概分為天然威脅、環境威脅、人為威脅及系統威脅。
- 天然威脅屬於不可抗力因素所造成，包含：水災、地震、颱風及土石流。
- 環境威脅包含：火災、長期停電、污染及治安問題。
- 人為威脅包含：打錯資料、誤刪檔案及踢到插頭等無意的行為，或是竊盜、惡意破壞及放置後門程式等有意的行為。
- 系統威脅包含：硬碟壞軌、當機及網路中斷。
- 舉例：
  - SARS與H1N1這兩種法定傳染病屬於哪一種威脅？Ans：環境威脅。
  - 未授權存取設備屬於哪一種威脅？Ans：有意的人為威脅居多，因為並未授權人員可以存取。當然也不 能排除是無意的行為，因人員不知道他沒有存取權限。
  - 駭客屬於哪一種威脅？Ans：有意的人為威脅。



- 脆弱性的種類大致分為技術類、操作類及管理類。
- 技術類的弱點有：設計不良與系統漏洞等。
- 操作類的弱點有：習慣不良與缺乏備份等。
- 管理類的弱點有：制度不良與缺乏管理等。
- 通常技術類的弱點可以透過下列幾種方法鑑別出來：
  1.自動化的脆弱性掃瞄工具。
  2.安全性測試與評估。
  3.滲透測試。
  4.程式碼審查。
- 操作類與管理類弱點則可透過下列方式鑑別出來：
  1.與人員、使用者晤談。
  2.問卷調查。
  3.實體檢查。
  4.文件分析。

鑑別脆弱性

- 脆弱性資訊的蒐集方式
  - 現場調查
  - 運用弱點掃描工具
  - 檢視系統與組織的文件
  - 檢視系統廠商提供的脆弱性資料
  - 於系統未設計時，注意安全政策、措施及系統需求定義
  - 於系統正在開發時，則注重較特定的部分。如：設計文件
  - 於系統已上線時，則分析既定的安控功能或安控機制執行的成效

脆弱性資訊的蒐集方式：

1.現場觀察到有一些民眾身分證資料被丟棄在資源回收箱、印表機上留有機密文件未取走、離座同仁桌上有機密公文黃色卷宗夾、離座同仁座位有同事個資聯絡資訊、進出檔案室或機房時不會隨手關門等，透過現場觀察，可以發現機關同仁有資安認知不足的脆弱性。

2.透過弱點掃描工具，也可以知道存在什麼樣的脆弱性。

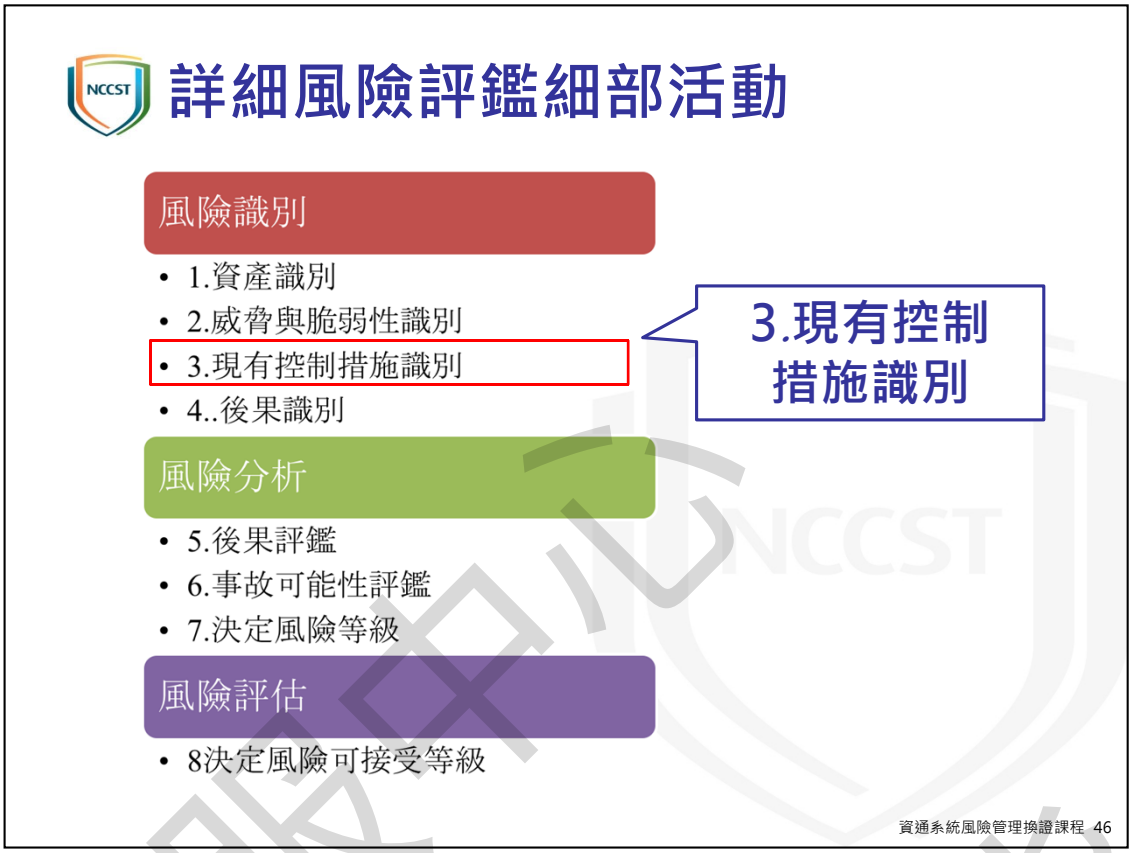
3.檢視系統與組織文件(例如：系統管理手冊或系統規格書)也可讓有心人士輕易了解組織的脆弱性。

4.委由廠商執行弱點掃描或滲透測試，廠商所提供的掃描報告忠實反映出機關現有的脆弱性，若此報告外流，有心人士就可依此報告攻擊組織的弱點。

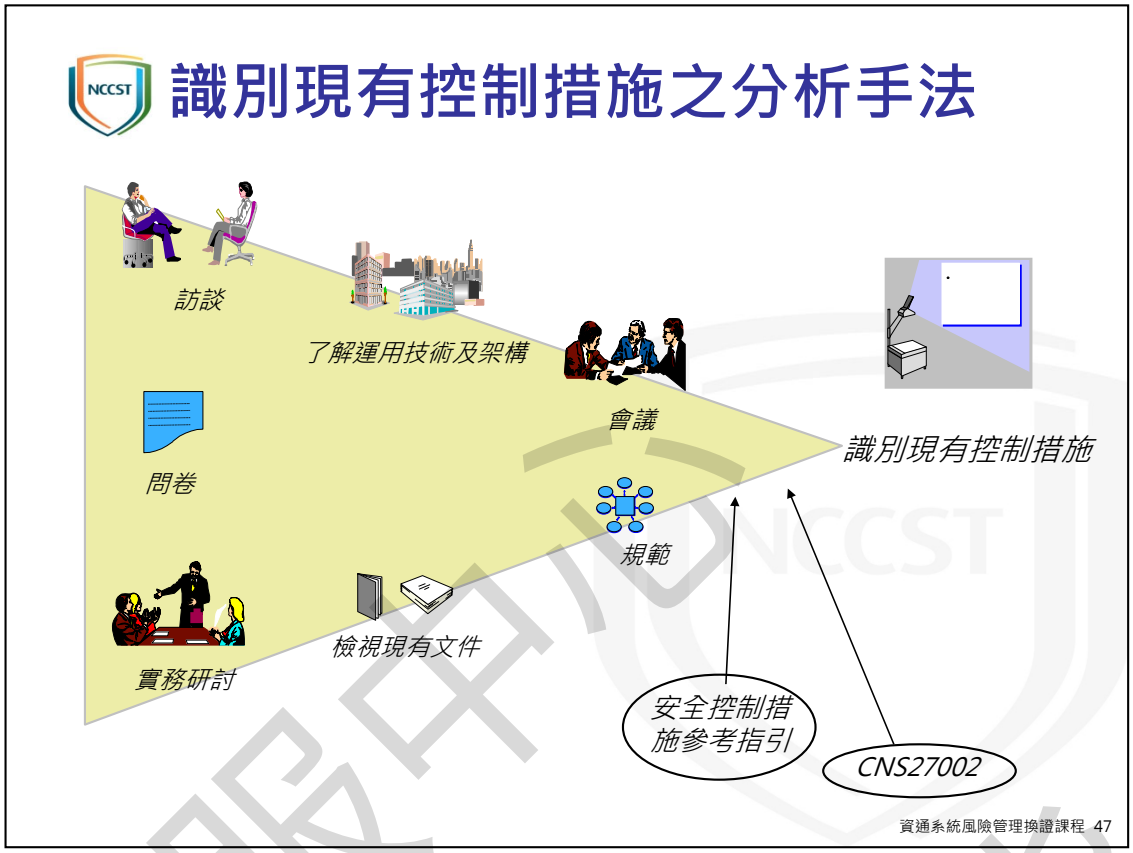
5.系統委外開發還未進入設計階段，尚在需求確認階段就應著重有何安全需求(例如：廠商交付程式不得有惡意程式碼且必須附上源碼檢測報告；系統應設計應用系統日誌功能，以利稽核個資的存取行為；列印或查詢功能宜適度對個資做遮罩或侷限大量匯出個資的功能等），儘早提出需求讓廠商有所因應，免得進入開發階段後才要補強，所耗費人力預算更可觀。這樣的需求也可鑑別出是否有脆弱性。(例如：委外開發的系統明顯有個資，但未提及任何日誌功能或遮罩個資的功能需求，就可知該組織明顯有很大的脆弱性存在，未善盡對個資保護之責）。

6.進入施工開發階段，要對系統設計規格書與系統分析規格書這類文件要求即時更新且詳實說明，上述文件不齊備或未更新，系統容易發生程式bug之類的問題，且程式設計師沒有可以參考的文件，無法了解系統的整體架構，日後若有需要修改程式，將會十分困難。

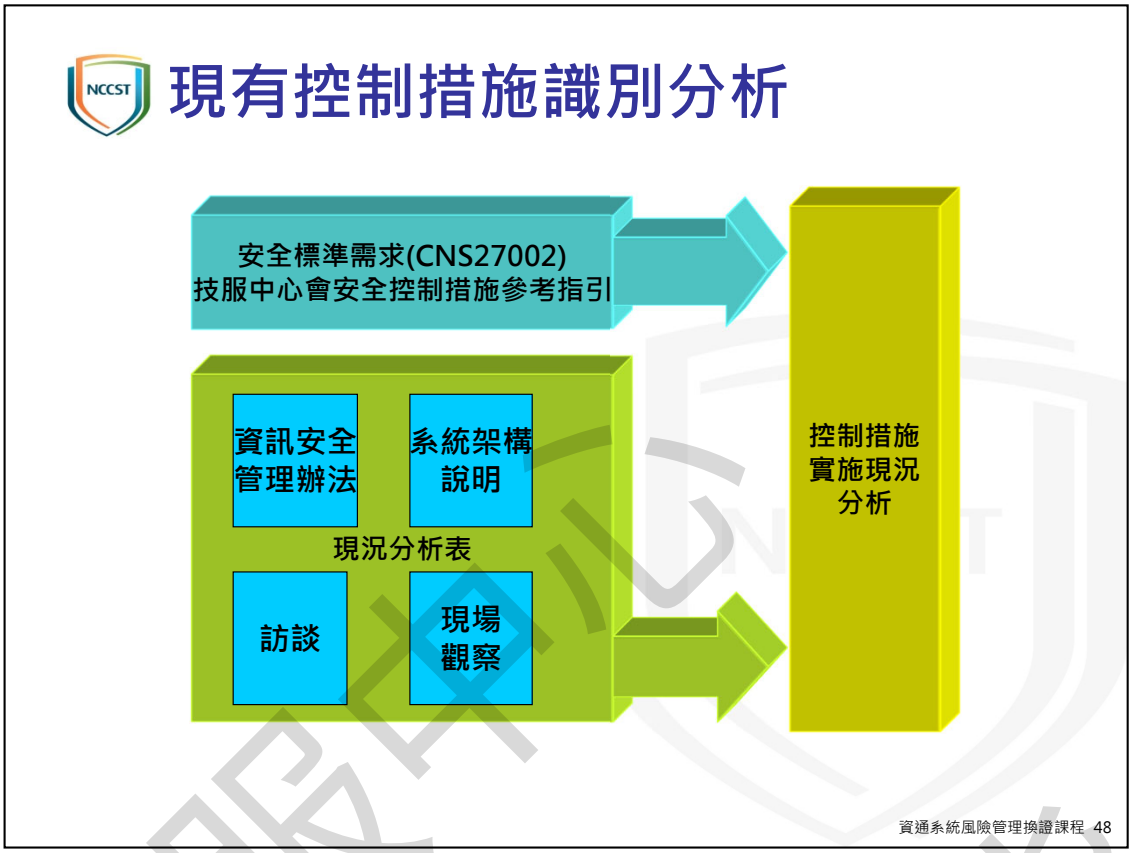
7.系統上線要著重如何上線的過程：廠商可不可以在正式機上修改程式？廠商有沒有提交測試報告？有沒有測試環境？如何管控原始程式碼的版本？廠商可不可以遠端連線做上線動作？上線過程有沒有人陪同受到監控？諸如此類，只要檢視上線的進行方式與安控措施，就可了解組織有什麼脆弱性。



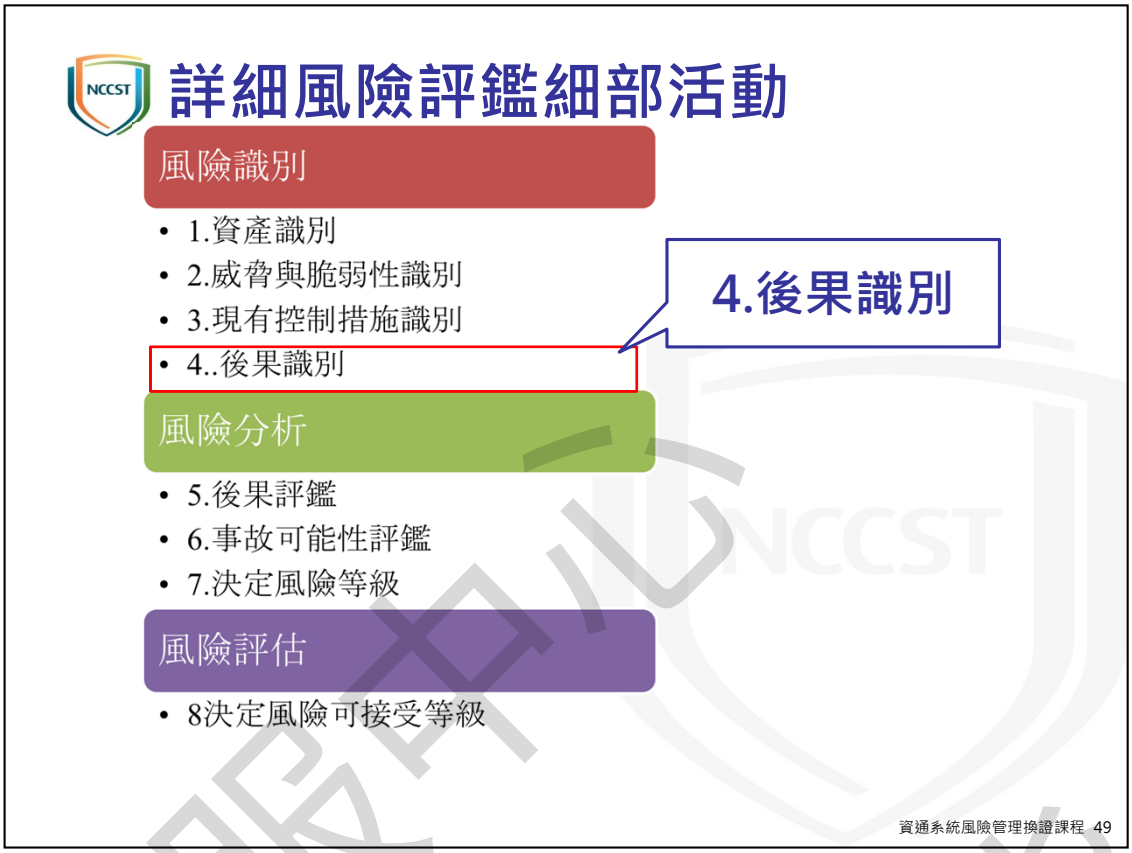
- 現在說明詳細風險評鑑的第3個步驟現有控制措施識別



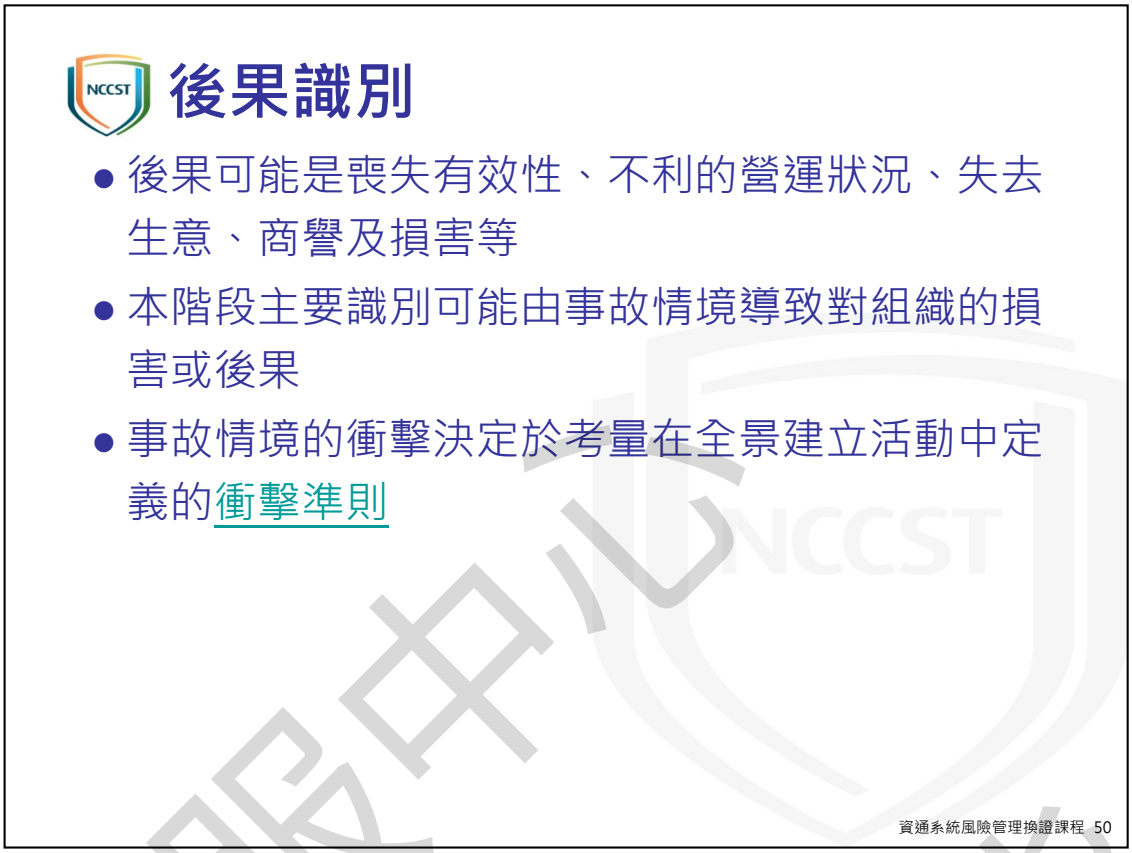
- 如何識別出現有安控措施，可採用的方式有：
  - 透過訪談了解；
  - 問卷調查；
  - 透過實務研討了解；
  - 檢視現有文件了解運用技術與架構；
  - 會議；
  - 規範文件。
- 機關若要通過CNS 27001，務必要參考附錄A選擇適用的控制措施。而有關附錄A的最佳實務作法就要參考CNS 27002。
- 安全控制措施參考指引也是識別現有控制措施時可以參考的重要文件。
- 識別現有控制措施的進行方式有以下幾種做法：
  - 收集安全管理資訊，包括：安全要求的期望、安全組織運作、安全管理措施(管理面)落實程度及安全管理措施實施之有效性。
  - 系統安全措施與運作說明。
  - 現有文件與管理辦法檢視，以了解現行控制措施。
  - 現場觀察。
  - 訪談。
  - 利用工具：業務流程分析表指的是將流程方法(process approach)由輸入到輸出的過程，將使用到的資源，規範及產出紀錄，以Excel表格呈現的一份表單，有助於了解系統或業務流程作法。
  - 現況分析表指的就是將CNS 27001附錄A條款列出，一一訪談機關現已採行的安控措施，並記錄各條款現行作法的一份文件。



- 使用CNS27002與安全控制措施參考指引，透過訪談、現場觀察、檢視資訊安全管理辦法、系統架構說明及現況分析表，產出右圖的現有控制措施實施狀況，此即為現有控制措施識別分析。
- 識別現有控制措施的進行方式有以下幾種做法：
  - 收集安全管理資訊，包括：安全要求的期望、安全組織運作、安全管理措施(管理面)落實程度及安全管理措施實施之有效性。
  - 系統安全措施與運作說明。
  - 現有文件與管理辦法檢視，以了解現行控制措施。
  - 現場觀察。
  - 訪談。
  - 利用工具：業務流程分析表指的是將流程方法(process approach)由輸入到輸出的過程，將使用到的資源，規範及產出紀錄，以Excel表格呈現的一份表單，有助於了解系統或業務流程作法。
  - 現況分析表指的就是將CNS 27001附錄A條款列出，一一訪談機關現已採行的安控措施，並記錄各條款現行作法的一份文件。



- 現在說明詳細風險評鑑的第4個步驟後果識別



- 威脅與脆弱性識別出來後，與事故情境相結合，會導致機關的損害與衝擊，產生的後果可能是喪失有效性、不利的營運狀況或商譽受損等。
- 事故情境的衝擊決定於考量在全景建立活動中定義的衝擊準則，因此衝擊準則就十分重要，以財務損失程度作為衝擊準則或以影響範圍程度作為衝擊準則，甚至於以影響聲譽的程度作為衝擊準則都是可能的方式，重點是要訂出讓機關容易且可行的判斷準則。
- 以影響範圍程度訂定衝擊準則，是政府機關常見且可行的實施方式。

- 現在說明詳細風險評鑑的第5個步驟後果評鑑。

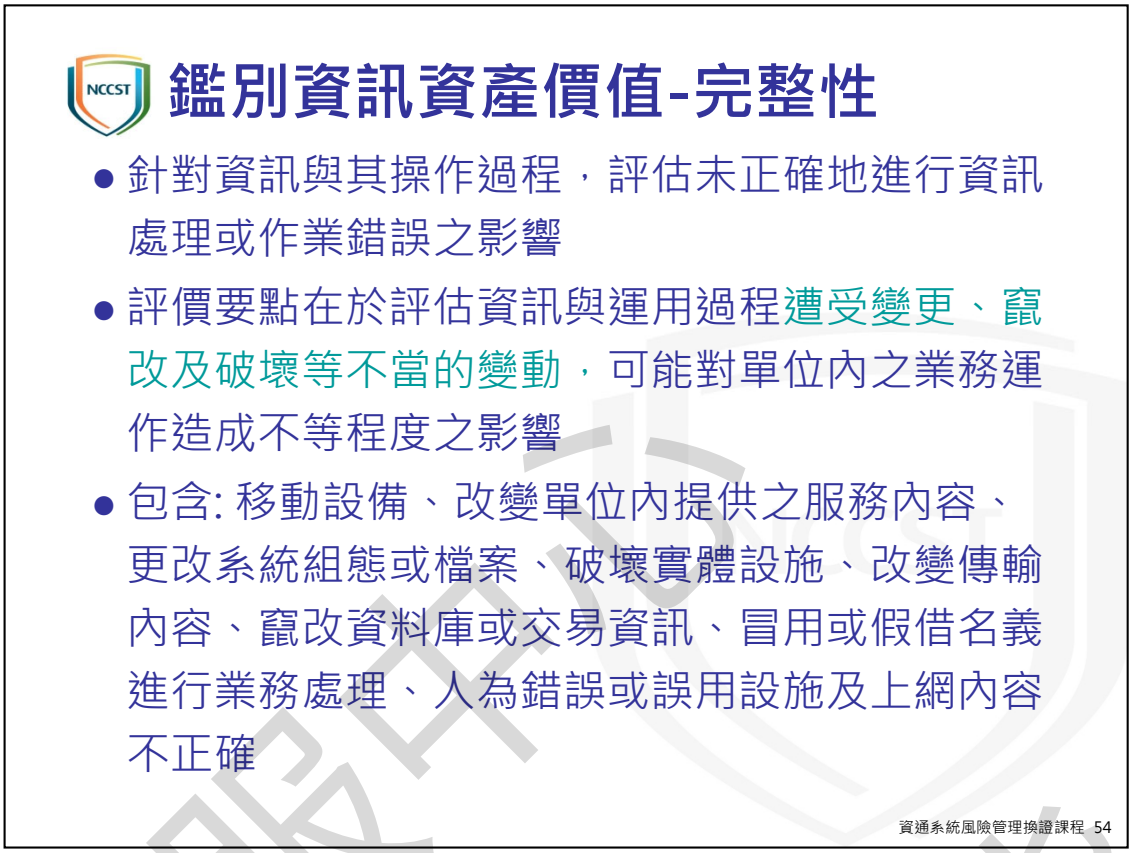
鑑別資訊資產價值-機密性

- 針對資訊與其使用權限分級要求，評估其未經授權存取之影響
- 評價要點在於資訊處理之授權，並且只有取得存取權限的人員或程序才可以進行授權範圍內之資訊的處理作業。未經過授權或不當的授權便進行資訊處理，可能對單位內之業務運作造成不等程度之影響
- 包含: 使用設備與單位內提供之服務、透露或複製經手之業務資料、存取資通系統及進入實體區隔之區域

- 鑑別資訊資產價值是針對資訊與其使用權限分級要求，評估其未經授權存取的影響。
- 評價要點在於資訊處理的授權，評鑑機密性喪失所造成的衝擊有多大。什麼是機密性喪失的狀況? 未授權存取就是一個機密性喪失的通案，因為機密性的定義為確保授權的人員方能允許存取資訊，因此，違反此準則就是指未授權存取。最能代表機密性的喪失。只有取得存取權限的人員或程序才可以進行授權範圍內的資訊處理作業。未經過授權或不當的授權便進行資訊處理，可能對單位內的業務運作造成不等程度的影響。包含: 使用設備與單位內提供之服務、透露或複製經手的業務資料、存取資通系統及進入實體區隔的區域。
- 人員的機密性喪失通常是指外洩。

機密性評等—範例

評等	說明
4	極機密：具有機密性之資訊資產，僅能開放給經過授權的人員使用。一旦洩漏，足以影響全機關整體聲譽及業務執行
3	機密：敏感性之資訊資產，僅能開放給經過授權的人員使用。一旦洩漏，足以影響各處室或專案之執行
2	內部使用：僅供內部使用，不可公開陳列之資訊資產。資訊遭洩漏，僅對個人之業務造成影響
1	普通資訊：非敏感性資訊資產，可公開使用者。資訊遭洩漏，不會造成影響或影響可忽略



- 鑑別資產完整性價值是指針對資訊與其操作過程，評估未正確地進行資訊處理或作業錯誤之影響。
- 評價要點在於評估資訊與運用過程遭受變更、竄改及破壞等不當的變動，可能對單位內之業務運作造成不等程度之影響。重點是指評鑑完整性喪失所造成的衝擊有多大，什麼是完整性喪失的狀況? 未授權竄改與破壞就是一個完整性喪失的通案。因為機密性的定義為確保資訊內容及資訊處理方法為正確而且完整，因此，違反此準則就是指未授權竄改與破壞，最能代表完整性的喪失。
- 包含: 移動設備、改變單位內提供之服務內容、更改系統組態或檔案、破壞實體設施、改變傳輸內容、竄改資料庫或交易資訊、冒用或假借名義進行業務處理、人為錯誤或誤用設施及上網內容不正確等。
- 人員的完整性喪失通常是指作業錯誤。

完整性評等—範例

評等	說明
4	極高:不當的破壞或篡改，會對全機關整體業務造成危害，甚至會造成業務衝擊者
3	高：不當的損失、破壞或篡改，會對各處室或計畫業務運作造成衝擊者
2	中：不當的損失、破壞或篡改，僅對個人造成衝擊者
1	低：遭受不當的破壞或篡改，其所造成的業務衝擊可以忽略者

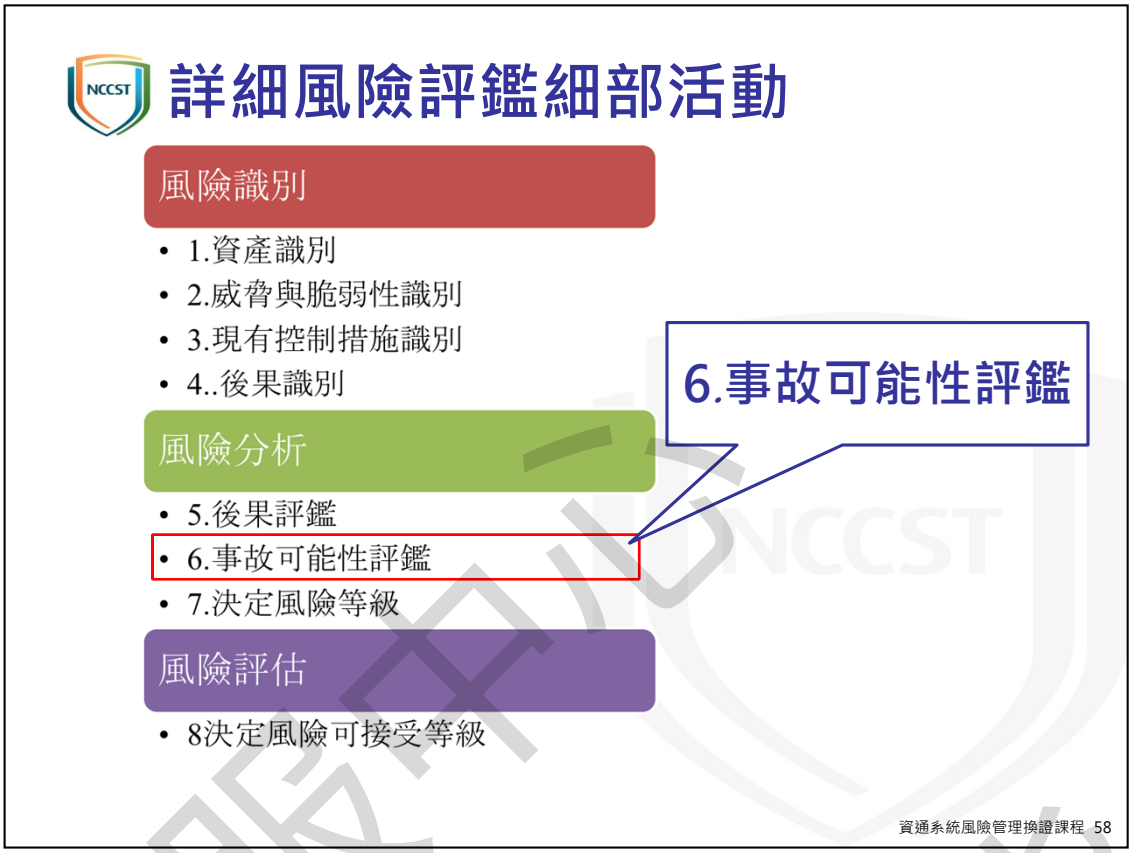
鑑別資訊資產價值-可用性

- 針對資訊與其處理過程，獲得適當授權者對於資訊與處理設備於需要存取時，評估無法正常使用的影響
- 評價要點在於評估其資訊運用過程中，提供正常服務的時間，被授權存取者無法使用資訊資產或無法執行業務，以程度區分對不同資產之需求
- 資產可用性喪失的情況如實體設施無法使用、實體區域無法進入、系統軟體或程式錯誤導致執行中斷、網路連線中斷、職務代理不明確及資通系統無法開啟

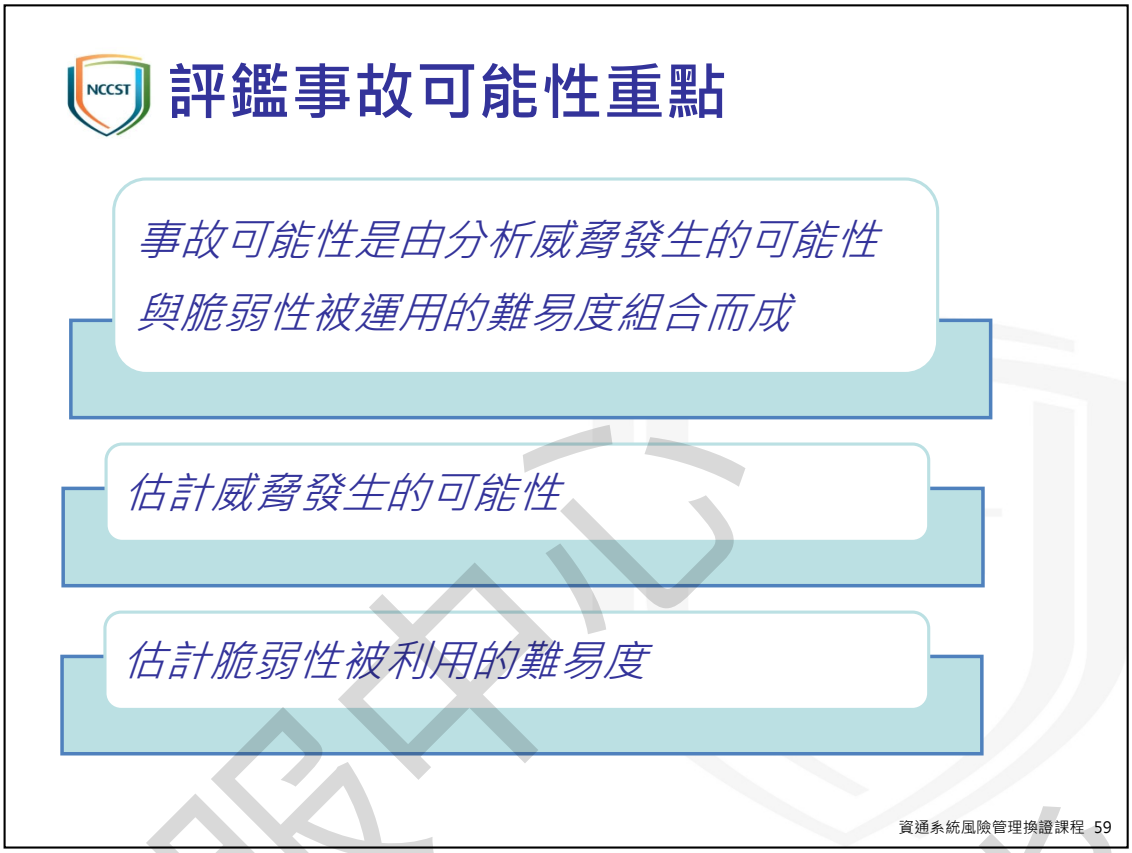
- 鑑別資產可用性價值指的是針對資訊與其處理過程，獲得適當授權者對於資訊與處理設備於需要存取時，評估無法正常使用的影響。
- 評價要點在於評估其資訊運用過程中，提供正常服務的時間，被授權存取者無法使用資訊資產或無法執行業務，以程度區分對不同資產之需求。重點就是指評鑑可用性喪失所造成的衝擊有多大。什麼是可用性喪失的狀況？故障或無法使用就是可用性喪失的通案。因為可用性的定義為確保經授權的使用者當需要時，能存取資訊與使用相關的資產，因此，違反此準則就是指無法使用，最能代表可用性的喪失。
- 資產可用性喪失的情況例如：實體設施無法使用、實體區域無法進入、系統軟體或程式錯誤導致執行中斷、網路連線中斷、職務代理不明確及資通系統無法開啟。
- 人員的可用性喪失通常是指人員無法執行業務時。

可用性評等—範例

評等	說明
4	極高：可用性遭受害，會對全機關整體業務造成危害，甚至會造成業務中斷者
3	高：可用性遭受損害，會對各處室或計畫業務運作造成衝擊者
2	中：可用性遭受損害，僅對個人造成衝擊者
1	低：可用性遭受損害，其所造成的業務衝擊可以忽略者



- 現在說明詳細風險評鑑的第6個步驟事故可能性評鑑



評鑑事故可能性重點是：

- 事故可能性是由分析威脅發生的可能性與脆弱性被運用的難易度組合而成。事故必須是威脅利用脆弱性結合產生，若資產有脆弱性，但無法被威脅所利用，則不會造成事故。
- 針對事故的可能性，將從威脅發生的機率(可能性)與脆弱性被利用的難易度這2個面向分別介紹。

威脅發生的可能性與評等

評等值	可能性評等	威脅曾經發生	威脅未發生過
3	高	每年發生6次(含)以上	事件或威脅沒發生過，但有可能發生且每月人為阻止每月4次(含)以上
2	中	每年發生1~5次	事件或威脅沒發生過，但有可能發生且人為阻止每月達1~3次
1	普	不太可能發生	事件或威脅沒發生過，但有可能發生且不太可能發生人為阻止事件

人為阻止：因為人為注意而阻止資安事件的發生
同時滿足多條件時，以滿足較高評等之條件為主
例：某威脅過去未曾發生(普)，但平均每月人為阻止三次(中)，因此可能性應評等為中(2)。

- 在設計區間時，儘可能以量化成數字為原則，避免訂發生機率「高」評3，發生機率「中」等評2，發生機率「低」評1，這類比較不明確的評鑑方式，畢竟高、中及低的差別見仁見智，若是能再細分到每年發生幾次算是高，每年發生幾次算是低，這樣就比較明確了。若區間不夠明確，會增加機關評鑑上的困難度。
- 威脅發生的可能性，可以從2個面向來看，1個是過去曾經發生的，1個是過去從未發生過的。
- 先從過去曾經發生這個面向來說，可藉由資安事件的統計了解過去發生了哪些事件，其所造成危害的資產為何？只要將其歸類到其資產即可。
- 但不能因為過去從未發生，就把威脅發生的機率評得非常低，還要看另1個面向才行，就是未來發生的可能性高不高。過去也許從未發生過資安事件，但在識別現有安控措施之下，還是得再評估未來有沒有可能發生，會不會是透過人為阻止方式，才降低事件發生機率。
- 這2個面向評鑑起來若有不同，要以較高評等做為最後的評鑑結果，把風險估高，以免日後實施的安控措施有所不足。
- 人為阻止的範例：辦公區存放機密件的櫃子未上鎖，從未發生機密件遺失事件，是因為有外人或廠商進到辦公室時，同仁都會幫忙詢問有什麼事，減少不相關人員逗留在辦公區的機會，因此而降低機密件遺失的情形發生。若這種情況經常發生，就應該把發生可能性評為「高」。

脆弱性被利用的難易度與評等

評等值	脆弱性評等值	難易度	說明
3	高	脆弱性很容易被利用	任何人不需具備任何能力均有可有意或無意的利用脆弱性
2	中	脆弱性被利用的難易度適中	具備瞭解脆弱性技術知識，方能利用脆弱性
1	普	脆弱性很難被利用	僅限深入瞭解脆弱性技術，並於特定條件或環境下方能利用脆弱性

使用者定義：
瞭解脆弱性技術知識：例如必須學過開鎖才能解鎖
深入瞭解脆弱性技術：例如必須瞭解系統內部設計架構，並學習過組合語言才能攻擊系統弱性
特定條件或環境：例如特定的作業系統、特定的時間及特定的操作方式

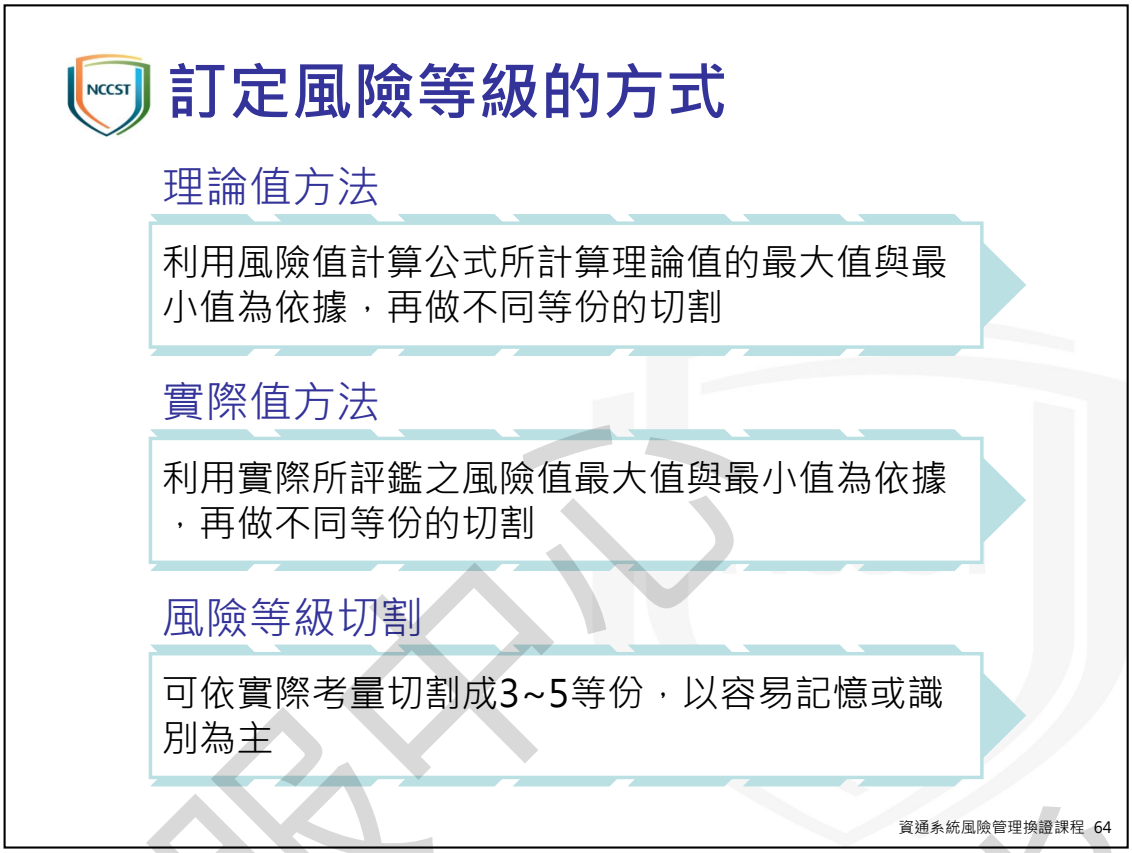
- 脆弱性的評鑑主要重點是看脆弱性容不容易被威脅所利用。如果容易，表示發生事件的機會較高，所以應評為高。
- 關於脆弱性，有多家顧問公司認為脆弱性很難評等，乾脆不評，而只對威脅做評等、識別出脆弱性是什麼而已。把脆弱性與威脅結合在一起評等也不能說是錯，但未必是好方法。學員應有分辨差異的能力。

- 現在說明詳細風險評鑑的第7個步驟決定風險等級。

訂定風險等級的目的

- 管理階層可輕易識別風險之高低
  - 解決管理階層不易由風險值判斷風險高低程度
  - 風險等級若分為高中普或分為ABCD等級，可輕易識別
- 做為可接受風險等級之決策參考
- 做為執行風險處理範圍之判斷依據
- 做為執行風險處理優先次序之判斷標準

- 由於經過公式計算，每項資產均有其風險值，要讓管理階層經由風險值的分數判斷是屬於高風險或低風險，有其困難度，因為不知道最高風險值是幾分。若再將各資產的風險值區分為3或4等分，以A、B、C、D或高、中、普這種方式表示，則管理階層很容易就能分辨該資產的風險是高或低，這也就是訂定風險等級最主要的目的。
- 例如：A級為不可接受風險，BCD級為可接受風險，做為可接受風險等級的決策參考。
- 也因為這樣的切割方式，可輕易讓管理階層判斷執行風險處理的範圍與優先次序，應該先針對A級或高風險投入人力與預算，以降低風險。



- 訂定風險等級的方式一般有理論值法與實際值法，理論值法是依理論值最大值與最小值為區間，切割成3或4等分；實際值法則是依實際評鑑的最大風險值與最小風險值為區間，切割成3或4等分來區分風險等級，2種方式各有優劣。
  1. 理論值法特性：若A是不可接受風險，因為理論值是固定的，所以，本次針對不可接受風險處理後，降低至可接受風險或殘餘風險，只要下次沒有出現A等級的風險，就不再另行執行風險處理計畫與量測KPI。
  2. 實際值法：假設本次最大風險值是72，72~3切割成4等分，先對最高等級A的資產執行相對應的風險處理計畫與有效性量測，半年後實際值最大值可能是60，再以60~3切割成4等分，再針對最高等級A的資產，執行相對應的風險處理計畫與有效性量測。按這樣的機制執行2年之後，大概機關可能的風險都可以有效掌控了。站在持續改善的精神，比較建議採用實際值法，可逐年提升機關的安全等級，降低機關的風險。

訂定風險計算公式(1/2)

- 資訊資產價值(公式範例)
  - (加法)機密性評價 + 完整性評價 + 可用性評價
  - (乘法)機密性評價 × 完整性評價 × 可用性評價
  - (加權法1)機密性評價 × 權重 + 完整性評價 + 可用性評價
  - 適用於關鍵業務處理著重機密資料或個資的機關/行業
  - 戶役政系統或入出境管理系統
  - (加權法2)機密性評價 + 完整性評價 + 可用性評價× 權重
  - 適用於關鍵業務著重提供可用性服務的機關/行業
  - 中華電信或宏碁IDC機房

- 估計風險等級的方式，一般都是透過內定的公式計算，因為前面已對資產做機密性，完整性及可用性評等，加上威脅與脆弱性評等，如此就可計算出風險值，估計風險等級。
- 但公式計算方式難有定論，不管用加法或乘法，各有其優劣。
  例如：資訊資產價值採用加法公式，原因為CIA這3項評等使用定性法分析方式，完全取決於評鑑者的判斷、經驗及直覺。若用乘法，由於定性法分析太過主觀，容易造成誤判，加上使用乘法，使得公式計算後更容易偏離實際情況。
- 風險值公式所舉範例取最大值法，係指取機密性評價、完整性評價及可用性評價之最大值後，再乘上威脅發生機率與脆弱性被利用難易度，此方法為多數驗證公司與學者所推崇，主要原因在於CIA是三個不同維度，對策自然有所不同，不宜相加。
- 而學者另外建議一種計算公式為分開計算法，即是機密性評價×威脅發生機率 × 脆弱性被利用難易度取1個風險值，完整性評價×威脅發生機率 × 脆弱性被利用難易度取1個風險值，可用性評價×威脅發生機率 × 脆弱性被利用難易度取1個風險值，分別針對不同風險實施對策。
  惟此方法須注意一點，若為機密性評價公式，則威脅識別時，應識別機密性喪失的威脅與脆弱性，否則，公式計算上會造成不合理現象。例如：機密性評價為設備遭未授權存取時，造成的衝擊程度為高，此資產威脅識別時，就不應識別當機或故障這類可用性喪失的威脅，否則分開計算法公式就會造成矛盾。實務上可能不易實施，因機關之風險評鑑小組可清楚識別威脅到底為機密性喪失或可用性喪失，若不透過工具選擇威脅與脆弱性，自行辨識恐有稍許難度。

訂定風險計算公式(2/2)

- 風險值(公式範例)
  - 資訊資產價值 × 威脅發生機率 × 脆弱性被利用難易度
  - (取最大值法)CIA評價取最大值 × 威脅發生機率 × 脆弱性被利用難易度
  - (分開計算法)機密性評價 × 威脅發生機率 × 脆弱性被利用難易度
- 須注意各種不同公式之運用差異，以挑選出最適合機關的風險計算公式

風險等級切割

- 風險等級可切割為不同等份，依機關或行業容易識別或記憶為主要考量
- 切割為3~5等份較適切
- 不須切割太細
- 機關建議作法：以切割為高、中及普三個等份為宜

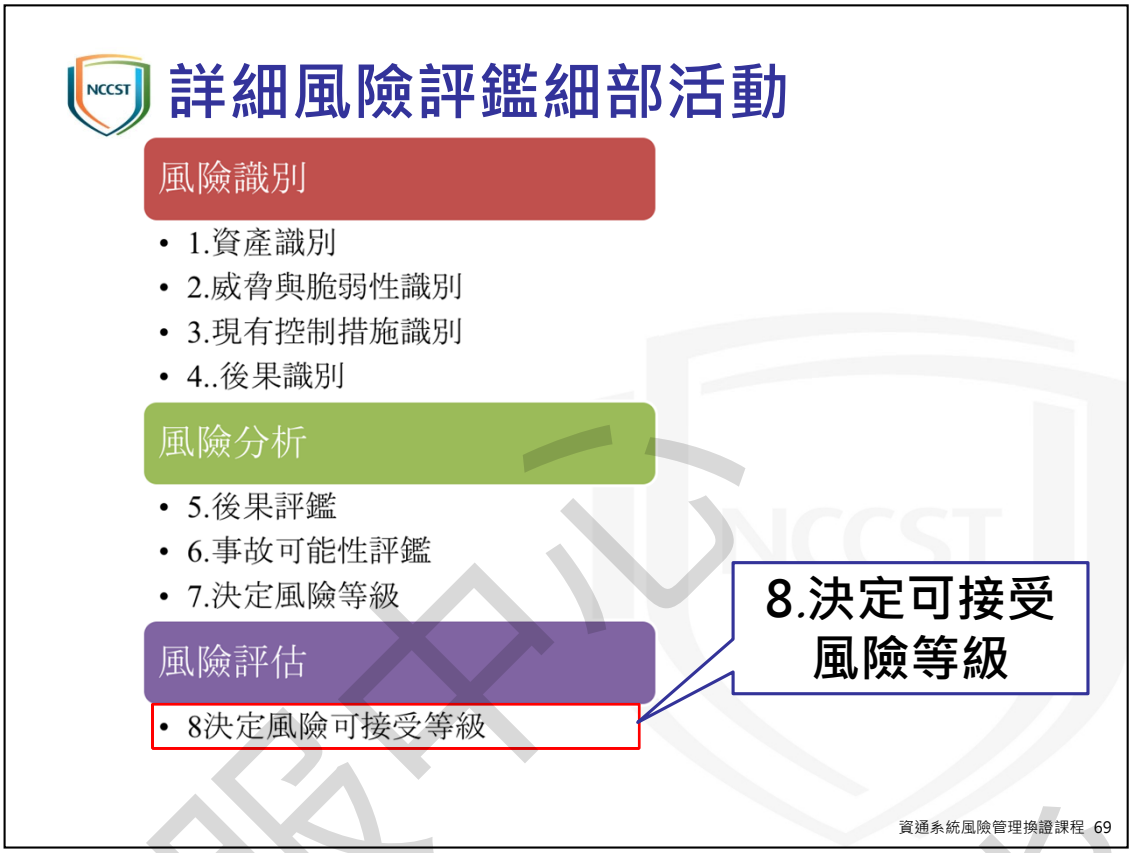
  (請參閱資通系統風險評鑑參考指引)

- 風險等級可切割為不同等份，依機關或行業容易識別或記憶為主要考量，一般建議切割為3~5等份較適切，不須切割太細，切割太細會造成究竟是最高的2個等級或3個等級為不可接受風險，等於是讓長官決策更複雜化。建議機關以切割為高、中及普三個等份為宜，容易銜接資通系統風險評鑑參考指引。

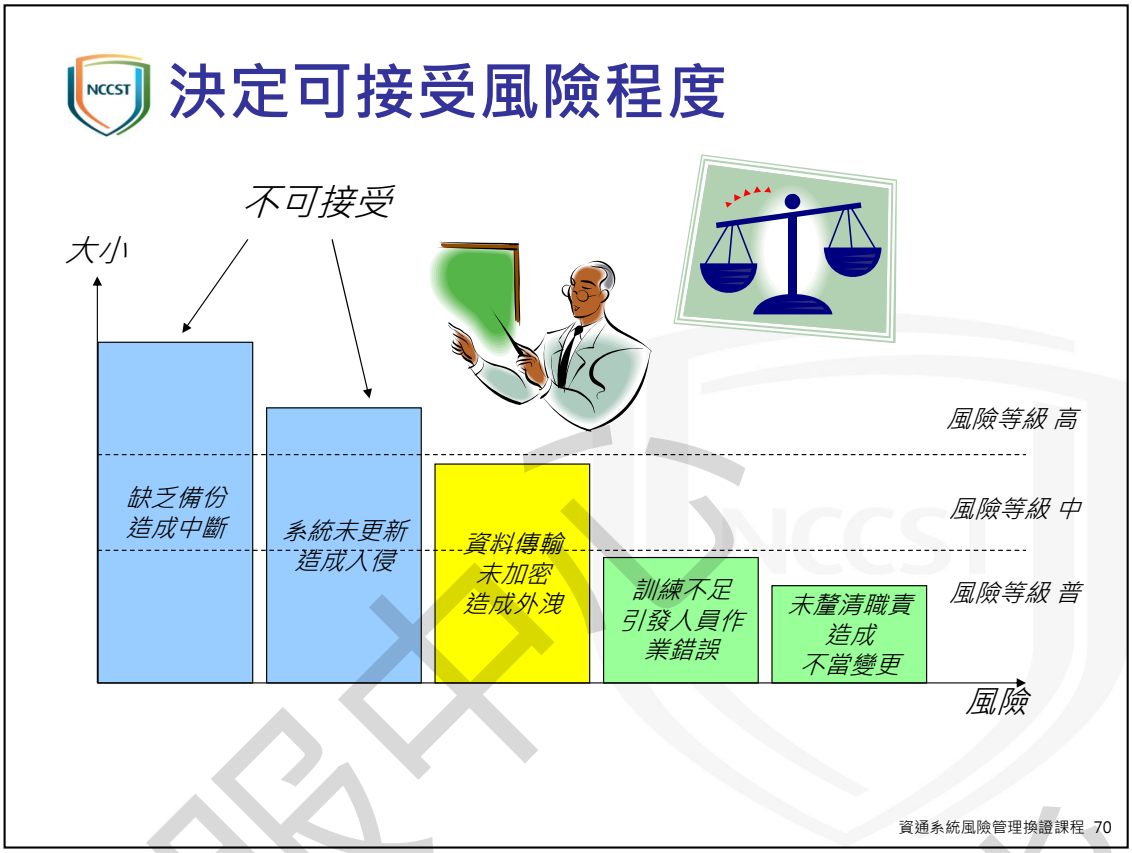
風險等級切割與機關既有作法轉換

- 步驟1：先決定採用理論值法或實際值法
- 步驟2
  - 若選用理論值法，依機關既有風險評鑑作法，計算出公式理論值最大值與最小值
  - 若選用實際值法，依機關既有風險評鑑作法，找出實際風險值的最大值與最小值
- 步驟3：將步驟2的最大值與最小值區間，切割為相同的3等份，依序定義為高、中及普，即完成風險等級轉換

- 現行A級與B級機關幾乎都已通過ISO27001驗證，因此機關已有既有的風險評鑑作法，可能區分為4或5個等級。將來行政院國家資通安全會報可能會要求各機關須依「資通系統分級與資安防護基準作業規定」對系統做高階風險評鑑，並回覆評鑑後的系統安全等級。該手冊區分為高、中、普3級，因此會有轉換既有作法的必要。
  - 步驟1：首先要決定採用理論值法或實際值法。
  - 步驟2：若選用理論值法，依機關既有風險評鑑作法，計算出公式理論值最大值與最小值；若選用實際值法，依機關既有風險評鑑作法，找出實際風險值的最大值與最小值。
  - 步驟3：將步驟2的最大值與最小值區間，切割為相同的3等份，依序定義為高、中、普，即完成風險等級轉換。



- 現在說明詳細風險評鑑的第7個步驟決定風險等級



- 若決定風險等級高為不可接受的風險，則必須對這2項藍色長條圖的資產，執行風險處理計畫與有效性量測，證明所採行的控制措施有效

決定可接受風險程度(範例)

- 風險值區間為1~10，決定風險值7(含)以上為不可接受的風險，7以下為可接受風險
- 風險等級區分為高、中及普，決定風險等級高為不可接受風險，風險等級中與普為可接受風險等級

- 風險值計算出來之後，依據建立全景階段所訂定的風險接受準則決定應該將不可接受風險訂在哪裡？
  簡單地說，假如風險值落在1分到10分，也許我們會訂6分以上或7分以上是不可接受風險；假如風險等級區分為高、中、普，決定風險等級高為不可接受風險，風險等級中與普為可接受風險等級，這完全取決於風險接受準則。機關依其業務特定決定哪個等級以上是不可接受風險，哪個等級以下是可接受風險。各機關切割不可接受風險與可接受風險的方式可能會有不同，這是因為每個機關都有自己的風險接受準則。

風險處理

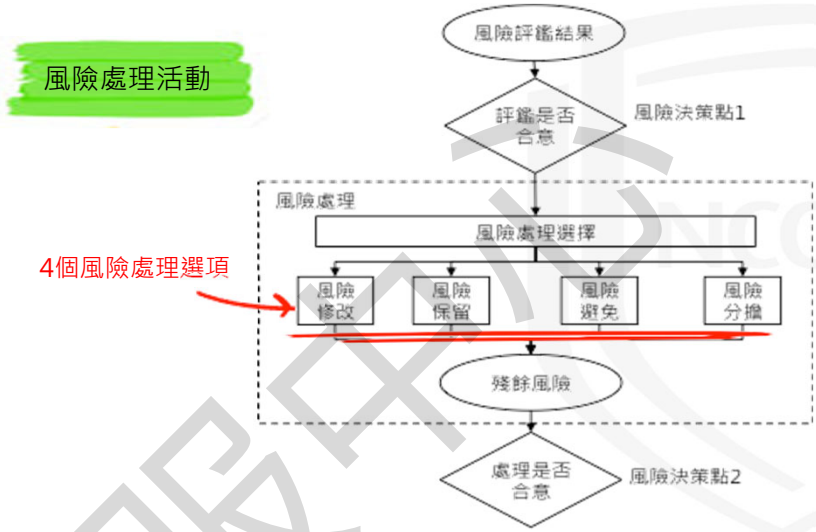
- 風險處理根據CNS14889的定義：選擇與實作措施的過程藉以修正風險。
- 風險處理的過程，是透過一系列的活動所產生的結果。
- 由於風險的產生，是威脅利用脆弱點，對有價值的資訊資產造成機密性、完成性與可用性三個層面的傷害，因此在風險處理的過程，首先就是要分析資訊資產本身的脆弱點為何，因為威脅沒辦法完全消失，僅能減少其發生的機率。透過脆弱點的分析，選擇強化脆弱的策略之後，就可以進一步選擇控制措施，這一連串的過程就是風險處理。

例如：

- 筆記型電腦輕巧，外人進入時容易被偷走。強化脆弱點的方式：增加筆記型電腦鎖，將筆記型電腦鎖在大型傢俱上，讓有心人士無法偷走。
- 應用系統常因程式寫法問題，造成資料庫鎖死。強化脆弱點的方式：修改程式語法，避免因程式語法鎖住資料庫而使應用系統無法執行。

風險處理

- 風險處理活動，應依據風險評鑑結果、實作風險處理方案之預期成本及預期利益等，選擇適當行動方案
- 一般而言，宜使風險不利後果合理的降低



- 風險處理是風險評鑑後的第一個工作，不論是高階風險評鑑或詳細風險評鑑，都要執行風險處理與風險接受這兩個階段。風險評鑑是找出目前所面臨的風險在哪，而風險處理則是運用一些措施讓風險降到可接受的風險。風險處理活動選項，主要有 4 種：風險修改(風險降低)、風險保留(風險接受)、風險避免及風險分擔
- 參考CNS 27005

控制措施選擇原則

選擇控制措施之原則

- 選擇控制措施之依據
  - –ISO/IEC 27001附錄A
  - –安全控制措施參考指引
- 控制措施之整理
  - –確認控制措施之完整性
  - –確認關照到所有的威脅與脆弱性
  - –評估與考量：在控制措施的成本與風險之間取得平衡

- 風險處理策略僅是在思考控制措施時的一個選擇方向，透過4個層次的思考方式決定下一步的控制措施，控制措施才是真正的執行風險處理的手段，因此要如何選擇控制措施才是最重要也是最難的部份，選擇控制措施的原則，可以參考ISO/IEC 27001附錄A或安全控制措施參考指引。

控制措施選擇的基本概念：

- 控制措施選擇的方式先要決定風險處理的選擇策略，包括：風險降低、風險轉移、風險避免及風險保留，決定要用什麼方式進行風險的處理。選擇好策略後，再選擇用什麼類別的控制措施，是行政管理類、技術類或實體類，最後再決定控制措施選擇的基本概念。
- 控制措施選擇的基本概念，主要是根據控制措施的用途做區分，分為預防、偵測、回應及復原，大部份的控制措施都是以預防為出發點。

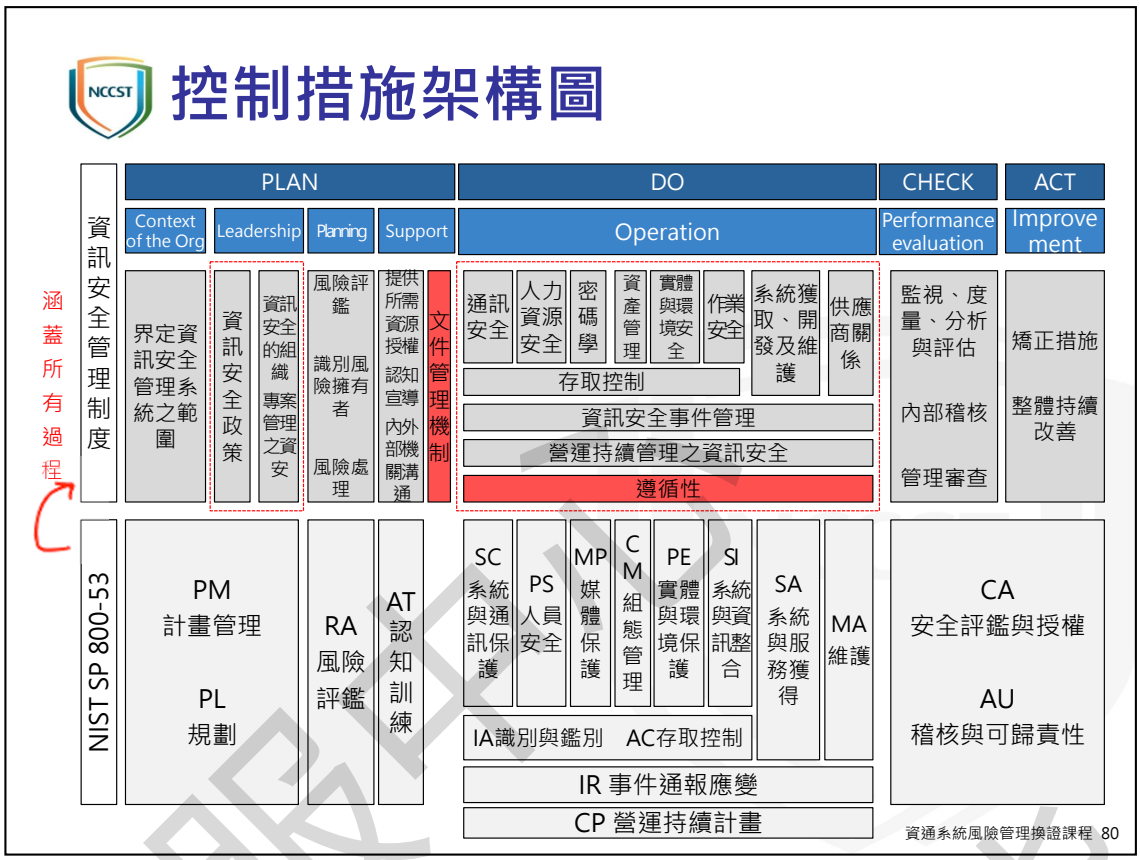
安全控制措施參考指引介紹

安全控制措施參考指引

- 控制措施分類架構

  融合CNS 27001 (14個領域，35個類別，114個控制措施)與NIST-SP800-53 Rev4 (18類，共240項)進行分類

- 使用指南
  - 先依「資通安全責任等級分級辦法」將資通系統安全等級區分為「普、中、高」3級 ← 高階風險評鑑作法
  - 再依該系統等級，參考「安全控制措施參考指引」的「安全控制措施」，選擇適用的項目



- 世界各國為提供各級政府機關，建議的安全控制措施，通常會依據重要性、組織規模及業務類型分組，區分不同安全等級，並建議適用的安全控制措施，或更進一步建議控制措施所適用的安全等級或優先順序
- 為便於理解與比較，將 NIST SP800-53 rev4，參考 PDCA與高階架構 (high level structure)關係，與 CNS 27001架構比較，兩者差異處，以紅色醒目標示
- NIST SP800-53 rev4 總計 18 類，共計 240 項控制措施，內容涵蓋 CNS/ISO/IEC 27001所有過程
- 關鍵在於 CNS 27001 供第三方驗證標準，NIST SP800-53 rev4 供聯邦政府機關參考之控制措施建議
- 故NIST SP800-53 rev4 架構未見「文件管制機制」與「遵循性」要求，在其他文件另外要求
- 而NIST SP800-53 rev4 除了提供控制措施建議外，並針對所有控制措施，區分為普、中、高3級，亦建議控制措施執行的優先順序
- 詳細內容，請參閱「安全控制措施參考指引」

高階風險評鑑作法（選擇初始安全控制措施）

機關於資通系統風險評鑑階段採用「高階風險評鑑」方法，對於資通系統之風險等級或是安全等級進行評定後，可右表之建議來選擇資通系統「普」、「中」、「高」應實作之安全控制措施。

控制措施	安全等級			參考文件
	普	中	高	
存取控制(Access Control)(3)				
帳號管理 (Account Management)	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。	1. 執行等級「普」之所有控制措施。 2. 資訊系統已逾期之臨時或緊急帳號應刪除或禁用。 3. 應禁用資訊系統閒置帳號。 4. 應定期審核資訊系統帳號之建立、修改、啟用、禁用及刪除動作。	1. 執行等級「中」之所有控制措施。 2. 當超過機關所規定之預期閒置時間或可使用期限時，系統應自動將使用者登出。 3. 資訊系統應依照機關所規定之情況及條件(如上班時間或指定 IP 來源)，使用資訊系統。 4. 監控資訊系統帳號以發現違常使用，並於發現帳號違常使用時回報管理者。	安全控制措施參考指引附件 4 AC-2
最小權限 (Least Privilege)		1. 採用最小權限原則，只允許使用者(或代表使	執行等級「中」之所有控	安全控制措施參考指引附件

資通系統風險管理換證課程 81

- 高階風險評鑑完成後，會依資通系統等級評估出普、中、高三種等級，再依各等級的方式列出初始的安全控制措施。如圖，高階風險評鑑評估出來後為普級，藍色框線部份即為初始安全控制措施的選定。

詳細風險評鑑作法 (選擇初始安全控制措施)

資通系統
風險評鑑
參考指引
(詳細風險評鑑)

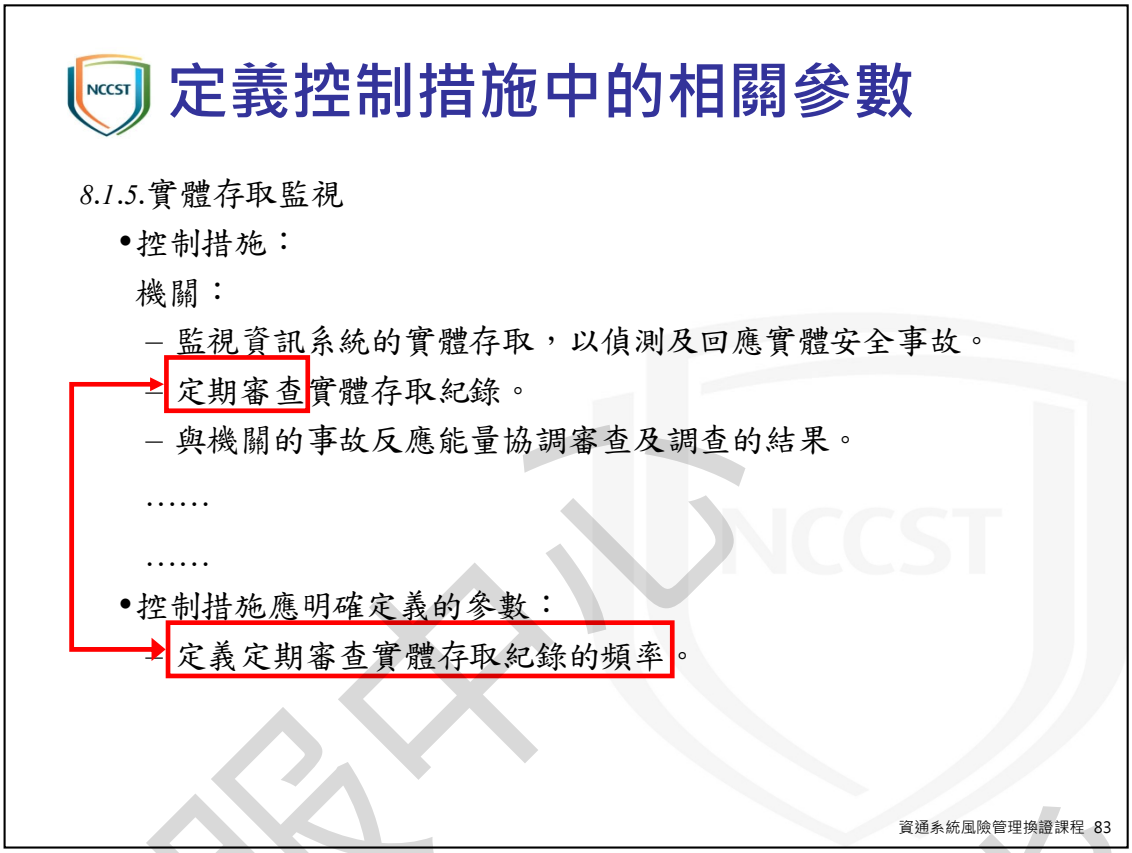
詳細風險評鑑報告
(風險需處理項目)

資產	威脅/弱點/可能性	風險
A	X.....	10
B	X.....	8
C		7
..	...	..
X	X.....	5

編號	名稱	是否選用	選用/不選用原因
安全政策與程序			
4.1.1	資訊安全政策文件	□是 □否	
4.1.2	資訊安全程序文件	□是 □否	
4.1.3	審查資訊安全政策及程序文件	□是 □否	
組織資訊安全			
5.1.1	系統安全規劃	□是 □否	
5.1.2	行為的規則	□是 □否	
5.1.3	隱私權影響評鑑	□是 □否	
5.1.4	安全相關活動規劃	□是 □否	
資產管理			
6.1.1	基準組態	☑是 □否	因為...
6.1.2	組態變更控制	□是 □否	
6.1.3	安全衝擊分析	□是 □否	
6.1.4	變更之存取限制	□是 □否	
6.1.5	組態設定	□是 □否	
6.1.6	最小功能	□是 □否	
6.1.7	資通系統資產清冊	□是 □否	
6.1.8	組態管理計畫	□是 □否	

資通系統風險管理換證課程 82

- 詳細風險評鑑完成後，會依風險評估出較高的部份，優先選擇該單項的安全控制措施。



- 如何定義控制措施中的相關參數，如圖所示，「定期審查」是1個月、1季、半年還是1年，由各單位自行定義。在不同的控制措施裡會有不同的參數需要定義，因此，在選擇完控制措施後，需要確認一下每個控制措施，以確保參數都有被定義完成。

「選定」安全控制措施

編號	名稱	是否選用	選用/不選用原因
安全政策與程序			
4.1.1	資訊安全政策文件	☑是 ☐否	回應利害關係人期望
4.1.2	資訊安全程序文件	☑是 ☐否	規範程序確保安全
4.1.3	審查資訊安全政策及程序文件	☑是 ☐否	需由管理階層核准發行
組織資訊安全			
5.1.1	系統安全規劃	☑是 ☐否	規劃系統安全需求
5.1.2	行為的規則	☑是 ☐否	規範安全使用系統行為
5.1.3	隱私權影響評鑑	☐是 ☑否	業務未處理隱私資料
5.1.4	安全相關活動規劃	☑是 ☐否	規畫安全管理活動
資產管理			
6.1.1	基準組態	☑是 ☐否	設定安全組態基準
6.1.2	組態變更控制	☑是 ☐否	控管不安全變更
6.1.3	安全衝擊分析	☑是 ☐否	分析遭受安全衝擊影響
6.1.4	變更之存取限制	☑是 ☐否	防止非授權存取
6.1.5	組態設定	☑是 ☐否	管理組態以利快速回復
6.1.6	最小功能	☑是 ☐否	.....
6.1.7	資通系統資產清冊	☑是 ☐否	.....
6.1.8	組態管理計畫	☑是 ☐否	.....

- 最後依照初始選定之安全控制措施，並依範圍原則、補償性控制措施、補充其他所需控制措施、定義控制措施中的相關參數調整完後，再將所選擇的安全控制措施是否選用，填入安全控制措施選用清單中，並予以實作。

風險接受

風險接受(1/2)

- 輸入：受限於組織管理者接受決策的風險處理計畫與剩餘風險(出自CNS 27005)
- 風險處理計畫
  - 為管理資訊安全風險， 架構一項風險處理計畫，以識別適當管理措施、資源、責任及優先順序(CNS27001)
  - 描述如何處理已評鑑的風險以滿足風險接受準則(CNS27005)
- 剩餘風險(指風險處理後所剩餘的風險)
  - 取得管理階層對所提議之各項剩餘風險的核准(CNS27001)

- 要讓高階長官決定是否接受風險？必須有所依據，而所依據的來源(輸入)就是風險處理計畫與剩餘風險。
- 風險處理計畫，根據CNS 27001的定義，為管理資訊安全風險， 架構一項風險處理計畫， 以識別適當管理措施、資源、責任及優先順序。風險處理計畫必須被高階長官核准，且為驗證時之必要文件，缺乏本風險處理計畫即為主要缺失，無法通過驗證。
- 風險處理計畫執行後，透過有效性量測指標，證明所採行的安控措施可以有效地降低風險之後，此降低後的風險，即為剩餘風險，剩餘風險一樣要被管理階層所核准。

風險接受(2/2)

- 若其明顯的符合組織的政策與風險接受準則，則知悉與客觀地接受此等風險(CNS 27001)
- 對不能滿足風險接受準則的風險，建立有正當理由並接受之風險清單(CNS 27005)

- 是不是接受風險？端看其是否符合建立全景階段所訂的風險接受準則，如果符合，則可以客觀地接受此等風險。若不能符合風險接受準則，則應列出不符合風險接受準則的清單，並列出哪些是有正當理由而可接受的風險，哪些是執行風險處理計畫後而降低風險的。

風險變更

風險評鑑審查與變更管理時機

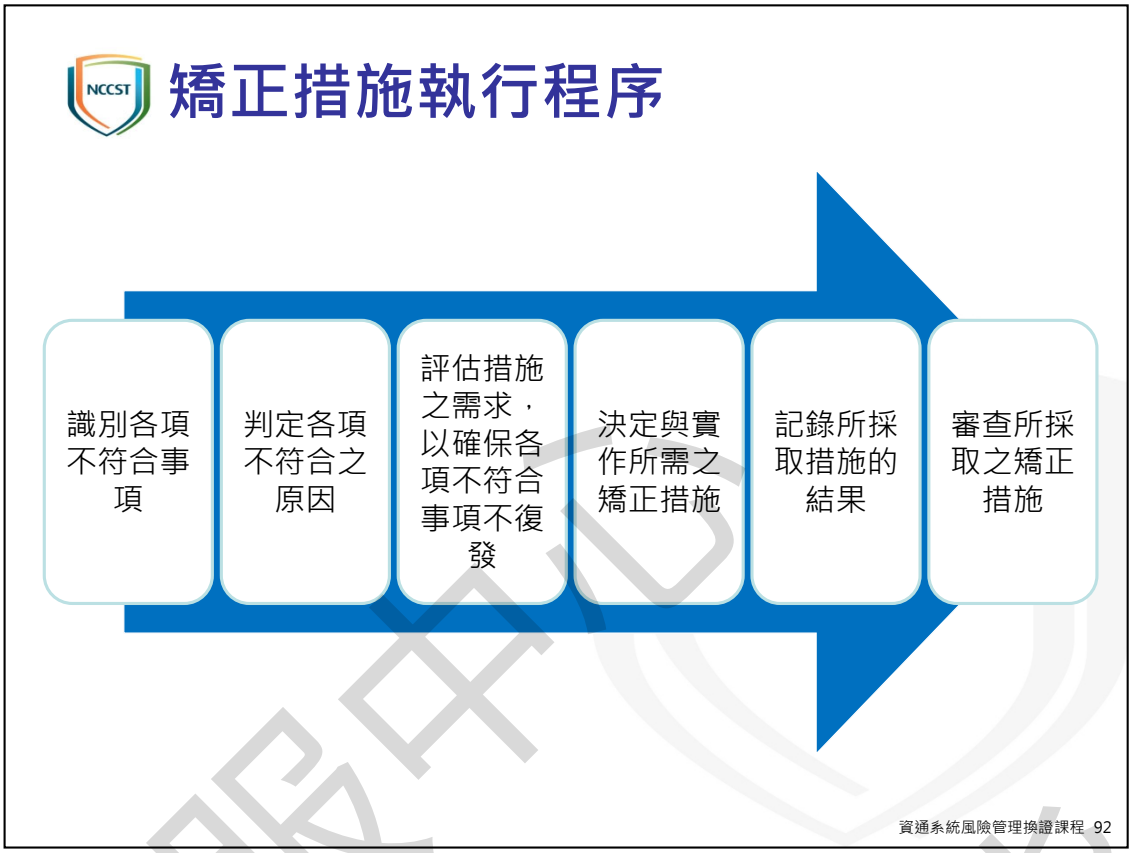
持續改進

持續改進

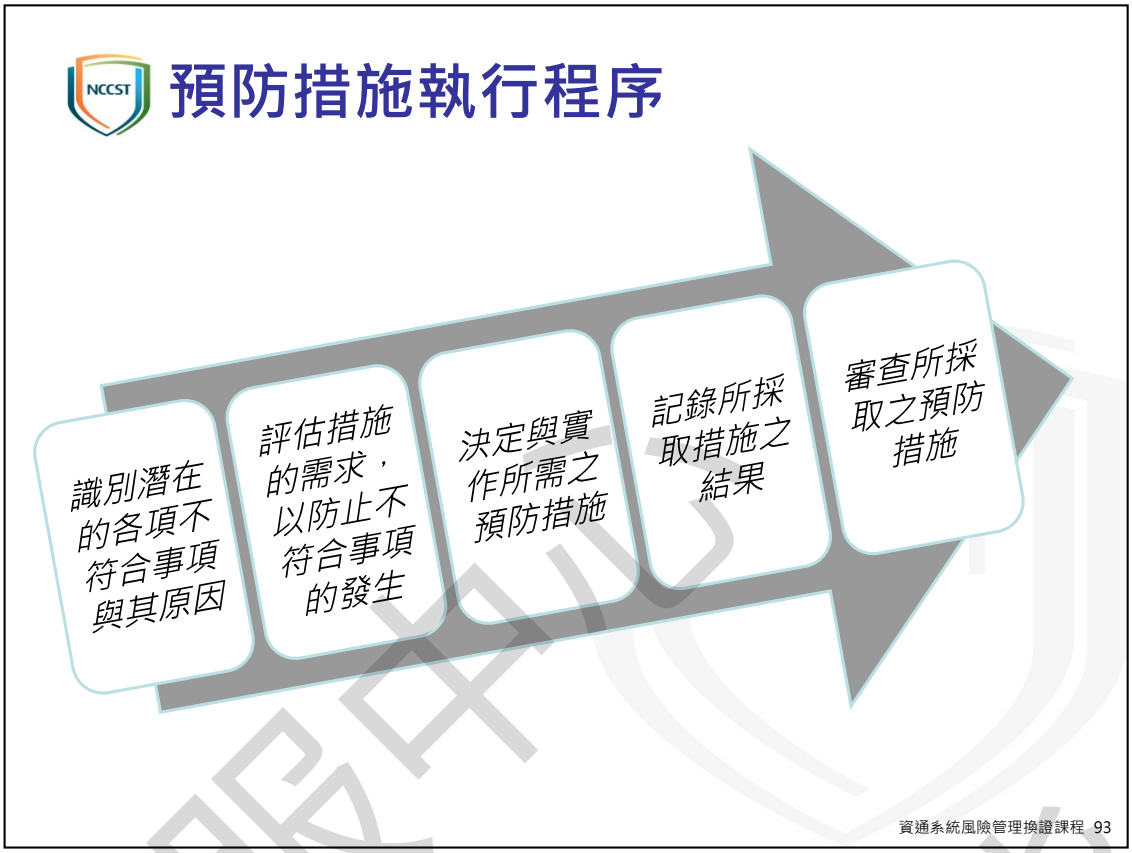
- 組織應藉由使用資訊安全政策、資訊安全目標、稽核結果、監視事件之分析、矯正與預防措施以及管理階層審查， 以持續改進ISMS之有效性
- 為了防止再發生， 組織應決定措施， 以消除與ISMS 要求不符合之原因
- 組織應決定措施， 以消除與ISMS 要求潛在不符合之原因， 並防止其發生。所採取之預防措施應與潛在問題之衝擊相稱

資料來源：CNS 27001

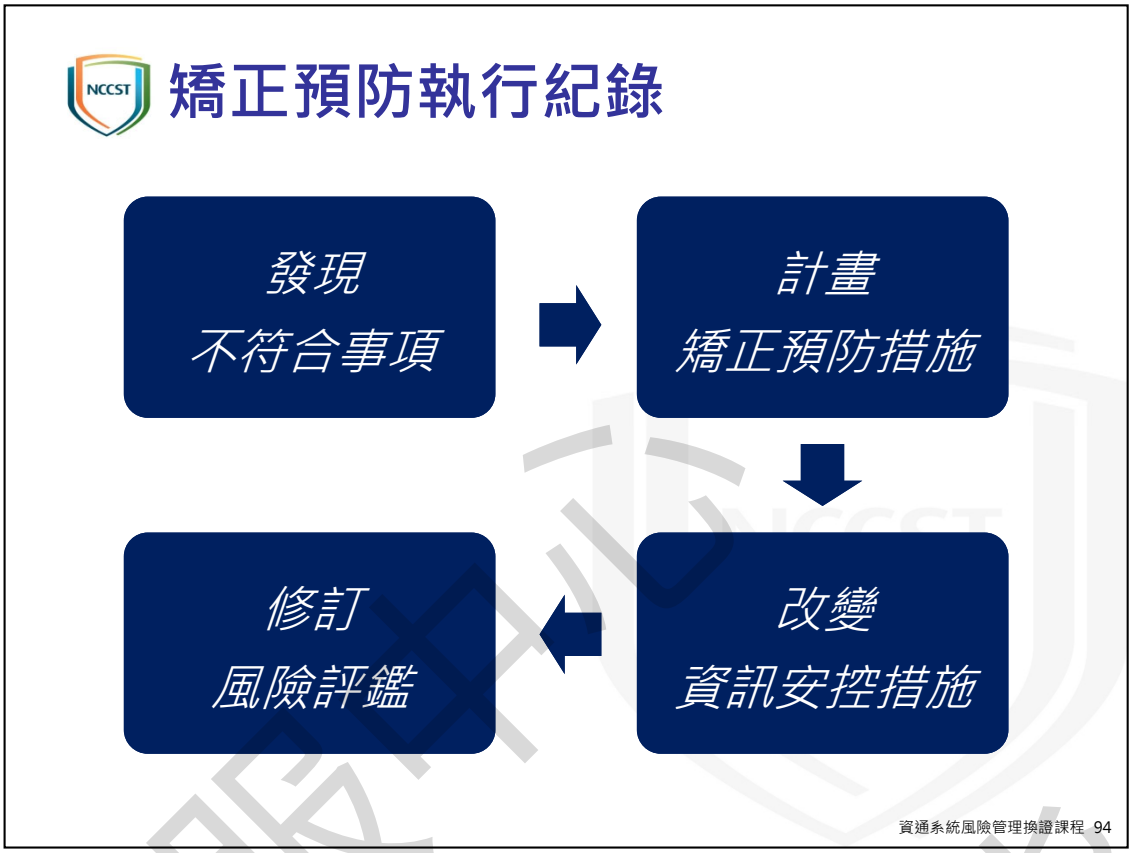
- 在風險管理流程中，應該依據「風險評鑑測試審查」階段所產生的結果，「持續改進」，並針對資通系統風險評鑑不符合或者需要調整改進的地方，採取必要的「矯正控制措施」與「預防控制措施」，以強化與落實資通系統風險評鑑的管理成效。
- 此外，依據ISO 27001對持續改進的要求，也應藉由資訊安全法令法規、資訊安全政策、內部稽核結果、監視資安事件之分析、矯正與預防控制措施並經權責主管審查，以持續並改進「執行風險評鑑」階段之有效性。
- 持續改進的作業中，機關為了防止風險或不符合事項再發生，應該針對不符合事項或需要改進的地方，找出發生的根本原因，針對原因決定相關措施， 以消除與ISMS 要求不符合之原因，這就是所謂的矯正措施。
- 為了防範未然，機關也應同時檢視潛在不符合與其原因，採取措施消除與ISMS要求潛在不符合之原因， 並防止其發生，這則屬於預防措施。所採取之預防措施應與潛在問題之衝擊相符合，也就是所選取的措施要能夠解決或預防潛在問題的發生。



- 為了防止資安事故或不符合事項再次發生，機關應決定矯正控制措施，以消除與資訊安全管理要求不符合之原因。矯正控制措施應以文件化程序記錄備查，並包含以下事項：
  1. 識別各項不符合事項—首先要確定不符合事項為何？如前面所說的，可能是資安事件發現的不符合事項需要改進以降低風險的狀況，或是由內外稽或管審會議發現的不符合事項。識別出事項後應該記錄於規定的表單中，並進行後續的矯正工作。
  2. 判定各項不符合之原因—接著就要進行最重要的工作之一，就是找出不符合事項發生的根本原因，請注意這個工作不是在描述事情發生的經過，而是將為什麼會發生這件事的原因找出來，例如：發生當機而造成服務中斷的事件時，我們不是只在描述當機的過程，而是要找出造成當機的原因，例如：記憶體不足或是硬體毀損的成因。
  3. 評估控制措施之需求，以確保各項不符合事項不復發—當找出根本原因之後，就要針對原因評估可行的控制措施並準備所需的資源，以消除這個根本原因。要注意所選的控制措施一定要能處理根本原因，而不只是解決表面的狀況。
  4. 決定與實作所需之矯正控制措施—當控制措施完成評估規劃後，應陳送相關主管同意後進行實作，同時也要定時進行追蹤與確認，對於未於期限內完成的矯正措施，應通知相關負責同仁注意執行的要求並及時完成措施。
  5. 記錄所採取控制措施的結果—對於所採取的控制措施、執行紀錄及其結果，都應該加以記錄，以便作為日後追蹤與效果驗證的依據。
  6. 審查所採取之矯正控制措施—對於矯正所採取的控制措施，應該在執行完畢後，審查措施的執行情形與效果是否達成預期目標，如果審查結果發現控制措施未能消除不符合事項再度發生的原因時，應該要求負責的同仁重新執行矯正措施。



- 在風險管理過程中，應根據「風險評鑑測試審查」管理程序中定期檢視風險評鑑控制措施的合適性與足夠性，以消除與資訊安全管理要求「潛在不符合」之原因，並防止其發生。所採取之預防措施應與潛在問題之衝擊相對應。
- 預防措施的執行程序應包括下列這些步驟：
  1. 識別潛在的各項不符合事項與其原因—與矯正措施的程序相似，首先要確定潛在不符合事項為何？這些潛在不符合事項是還沒有發生或尚未被發現的事項，但是在執行持續改善作業時，可能藉由討論或檢視相關事項，被識別出來。在識別出事項後應該加以記錄於規定的表單中，接著找出潛在不符合事項發生的根本原因。
  2. 評估控制措施的需求，以防止不符合事項的發生—做法與矯正措施相似，應該針對根本原因評估並規劃可行的控制措施避免不符合事項的發生。
  3. 決定與實作所需之預防控制措施—當控制措施完成評估規劃後，應陳送相關主管同意後進行實作，同時也要定時進行追蹤與確認，對於未於期限內完成的措施，應通知相關負責同仁注意執行的要求並及時完成措施。
  4. 記錄所採取控制措施之結果—對於所採取的控制措施、執行紀錄及其結果，都應該加以記錄，以便作為日後追蹤與效果驗證的依據。
  5. 審查所採取之預防控制措施—對於所採取的控制措施，應該在執行完畢後，審查措施的執行情形與效果是否達成預期目標，如果審查結果發現控制措施未能消除不符合事項再度發生的原因時，應該要求負責的同仁重新執行預防措施。



- 矯正預防執行過程中均應留下紀錄，這些紀錄不僅可做為持續改善的證據，也將做為修訂風險評鑑的重要資料來源。
  1. 發現不符合事項：
     我們所發現的各項不符合事項，均可做為風險評鑑中威脅或脆弱的資料來源，像是資安事件或是內外稽不符合事項，均應討論是否要納入本次的風險評鑑內容中。
  2. 計畫矯正預防措施
     矯正預防措施的提出與執行，會增加資訊安全管控措施或強化管控措施的強度，並減少脆弱性，這都應該反映在風險評鑑中。
  3. 改變資訊安控措施
     矯正預防措施會改變現有的資訊安控措施，所以在風險評鑑作業中，檢視安控措施時，應將這些改變納入考量。
  4. 修訂風險評鑑
     當這些變化影響了威脅、脆弱性及安控措施時，我們應該反映在風險值的改變，據以修訂風險評鑑結果。