國立中央大學電子計算機中心
「資訊安全管理系統顧問服務暨驗證範圍擴大案」

ISO27005概述

講師：吳昭儀

財團法人中華民國國家資訊基本建設產業發展協進會

課程大綱

- 資訊安全風險評鑑
- 資訊安全風險處理
- 資訊安全風險接受
- 資訊安全風險溝通
- 資訊安全風險監控與審查

課程大綱

- 資訊安全風險評鑑
- 資訊安全風險處理
- 資訊安全風險接受
- 資訊安全風險溝通
- 資訊安全風險監控與審查

何謂風險

- The chance of something happening that will have an impact upon objectives.
- 對於目標會產生影響的事件發生的機會。
  - 風險是未來的不確定事件，該事件會影響組織目標的達成，包括策略、作業、財務或其他目標。

資訊安全風險評鑑

資訊安全風險評鑑的一般描述 General description of information security risk assessment一般描述 General description of information security risk assessment

- 註 風險評鑑活動被稱為ISO/ IEC 27001 (CNS 27001）內的過程。
- 投入：要建立之資訊安全風險管理過程的基本準則、範疇與界限。
- 行動：宜識別、量化或以量描述、按風險評估準則和與組織有關的目標訂定優先順序。
- 實作指引：
- 風險是跟隨不想要事件所發生後果與該事件發生可能性的組合。風險評鑑量化或以量描述風險，並使管理者可依其所理解的嚴重性或其它已建立的準則訂定優先順序。
- 風險評鑑包括下列活動：
  - 風險分析含：
    - 風險識別
    - 風險估計
  - 風險評估
  - 產品、服務或機制資訊安全需求的描述
- 風險評鑑決定資訊資產的價值、識別現存（或可能存在）適用的威脅和脆弱性、識別現有的控制項目以及其對已識別風險的效果、決定看在後果、最後依全景建立中的風險評估準則訂定所導致風險的優先順序與排序。
- 風險評鑑通常會執行兩個（或更多）循環。首先執行高等級的評鑑以識別潛在且保護要進一步評鑑的高風險。下一循環得涉及對第一次循環顯示出的潛在高風險作更深度的考量。若未提供充分的資訊以評鑑該風險，則要執行更詳細的分析，也許是整個範疇的部份，也可能使用不同的方法。
- 由組織決定以目標和風險評鑑為基礎選擇其自己的風險評鑑方式。
- 附錄 E 有資訊安全風險評鑑方法的討論。
- 產出：一依風險評估準則訂定優先順序經評鑑後的清單。

風險分析-資產識別、威脅識別

資產識別

- 資產是對組織有價值的任何東西。
- 宜以適當等級的細節程度執行資產識別以提供風險評鑑的充分資訊。資產識別使用的細節程度將影響在資產評鑑中所收集的資訊整體數量。等級得在資產評鑑的下一循環中提昇。
- 宜識別每一項資產的擁有者，以提供該資產的職責和可歸責性。資產的擁有者可能沒有資產的財產權，但有其適當地生產、開發、維護、使用和安全等的責任。資產的擁有者通常是最適合決定該資產對組織之價值的人。
- 審查的界限是資訊安全風險管理過程所定義要管理的組織資產之周圍。附綠 B 有更多與資訊安全有關的資產識別與評估資訊。
- 產出：要被風險管理的資產清單，以及與資產及其關聯有關的業務過程清單。

威脅識別

- 威脅有潛在危害如資訊、流程、系統，故也危害資產。威脅可來自天然或人為，可能是意外或蓄意，宜識別意外與蓄意威脅的來源。威脅可由組織內或組織外引起。宜一般地與分類地(如：未經授權的動作、實體損害、技術失誤 ）識別各威脅，並於適當時在一般分類中識別出個別的威脅。這意謂包括未預期的威脅在內，沒有威脅會被忽略，但是可限制所需的工作量。
- 有些威脅可影響一項以上的資產。該種案例中它可依所影響的資產而導致不同的衝擊。
- 在目前的評鑑中宜考量來自事故的內部經驗與過去的威脅評鑑。在有相關時，諮詢其它威脅目錄（ 也許對組織或業務是特定的 ）以完成一般威脅的清單可能是值得做的。威脅目錄和統計資料可由產業團體、國家政府、法律組織、保險公司等取得。
- 在使用威脅目錄，或是先前威脅評鑑的結果時，宜認知到相關威脅的持續變更，特別是業務環境或資訊系統的變更。

風險分析-現有控制識別、識別脆弱性

現有控制識別

- 宜識別現有和已規劃的控制以避免不需要工作或成本，例如：複製的控制。此外，在識別現有的控制時，宜檢查以確保控制是正確地運作 - 已經存在 ISMS稽核報告的參照應可限制花費在此工作上的時間。若控制不如預期般運作，可能會導致脆弱性。宜考量營運中某一選定的控制(或策略)失敗，以致於需要補助的控制來有效地處理已識別的風險的情況。在 ISMS 內，依據ISO/ IEC 27001 (CNS 27001)，此部份由控制有效性的量測支援。
- 估計控制效果的方法之一是看其如何降低威脅的可能性並且減輕脆弱性的被利用，或是事故的衝擊。管理審查和稽核報告也提供關於現有控制有效性的資訊。
- 宜像已施行的控制一樣以相同方式考量依據風險處理施行計畫中已規劃將施行的控制。
- 現有和已規劃的控制可能被識別為無效果的，或不足的，或是不合理的。若是不合理或不足的，宜檢查該控制以決定是否要移除，替換為另一控制或更合適的控制，或者像以成本理由而言，是否繼續存在。

識別脆弱性

- 脆弱性的出現本身不會導致危害，因為需要有威脅來利用它。沒有相對威脅的脆弱性可能不需要施行控制，但宜在變更時識別與監控。宜注意不正確施行或機能失常的控制或被不正確使用的控制本身即是脆弱性。控制依其運作的環境可為有效或無效。相反的，沒有相對脆弱性的威脅可能不會造成風險。
- 脆弱性可與不是如當資產被購入或做出時所預期的使用的方式、或目的等特性有關。需要考量來自不同來源的脆弱性。

風險分析-現有控制識別、識別脆弱性

現有控制識別

- 宜識別現有和已規劃的控制以避免不需要工作或成本，例如：複製的控制。此外，在識別現有的控制時，宜檢查以確保控制是正確地運作 - 已經存在 ISMS稽核報告的參照應可限制花費在此工作上的時間。若控制不如預期般運作，可能會導致脆弱性。宜考量營運中某一選定的控制(或策略)失敗，以致於需要補助的控制來有效地處理已識別的風險的情況。在 ISMS 內，依據ISO/ IEC 27001 (CNS 27001)，此部份由控制有效性的量測支援。
- 估計控制效果的方法之一是看其如何降低威脅的可能性並且減輕脆弱性的被利用，或是事故的衝擊。管理審查和稽核報告也提供關於現有控制有效性的資訊。
- 宜像已施行的控制一樣以相同方式考量依據風險處理施行計畫中已規劃將施行的控制。
- 現有和已規劃的控制可能被識別為無效果的，或不足的，或是不合理的。若是不合理或不足的，宜檢查該控制以決定是否要移除，替換為另一控制或更合適的控制，或者像以成本理由而言，是否繼續存在。

識別脆弱性

- 脆弱性的出現本身不會導致危害，因為需要有威脅來利用它。沒有相對威脅的脆弱性可能不需要施行控制，但宜在變更時識別與監控。宜注意不正確施行或機能失常的控制或被不正確使用的控制本身即是脆弱性。控制依其運作的環境可為有效或無效。相反的，沒有相對脆弱性的威脅可能不會造成風險。
- 脆弱性可與不是如當資產被購入或做出時所預期的使用的方式、或目的等特性有關。需要考量來自不同來源的脆弱性。

風險估計-風險評估方法

附錄E　資訊安全風險評鑑方法取徑　範例 1 預設值矩陣

• 如下列範例矩陣所顯示的 0 到 4 級別，可在可能與合邏輯時能識別量的值，而在量的值不可能時識別質的值，如對人類生命的危害。

• 下一主要的活動是完成每一威脅形式、每一威脅形式相關的資產群組的配對問卷，以便能評鑑威脅等級（發生的可能性）與脆弱性等級（被威脅利用而導致不利後果的容易性）。每一問卷的回答帶來一個分數。這些分數經由知識庫累積並與各範圍比較。如此可同時識別比如說高至低等級的威脅等級與脆弱性等級，如下列範例矩陣所顯示的 0 到 4 級別，區分相關的後果形式。宜從晤談和合適的技術性、人事和設施的人員，實體的地點視察，和文件審查以收集可完成問卷的資訊。

• 資產價值，與威脅和脆弱性等級，相關於後果的每一形式，均配對於下面的矩陣，以識別每一相關 0 到 8 等級風險量測的組合。矩陣內以結構化的方式放置值。下面是一範例：

表E.1a

	發生可能性 – 威脅	低			中			高		
	易被利用	低	中	高	低	中	高	低	中	高
資產價值	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

課程大綱

- 資訊安全風險評鑑
- 資訊安全風險處理
- 資訊安全風險接受
- 資訊安全風險溝通
- 資訊安全風險監控與審查

風險處理概述

風險處理選項的選擇宜植基於風險評鑑的結果、施行該選項的預期成本與該選項的預期利益。

當風險上的大幅減低可以用相對低的花費而取得，此選項應予施行。更進一步的改善選項可能不經濟同時需要運用判斷以決定是否正當。

一般而言，宜使風險的不利後果盡量合理可行的低且與任何絕對的準則無關。

管理者宜考量稀有嚴重的風險。在該類案例中，可能需要施行純粹經濟理由不正當的控制(例如，業務持續營運控制被視為可涵蓋特定的高風險 ）。

風險處理的四個選項不是互相排外唯一的。有時組織得由如減低風險可能性、降低其後果與轉移或保留任何剩餘風險等的選項組合而大量獲益。

部份風險處理能有效地處理不只一項風險（ 如資訊安全訓練與認知 ）。宜定義風險處理計畫，依個別風險處理的施行與其時問範圍清楚地識別排列出優先順序。可使用不同技術建立優先順序，包括風險分級和成本效益分析。決定控制的施行成本和預算任務問的平衡是組織管理者的責任。

在成本比較方面，識別現有控制可決定現有控制超出包括維護的現有需求。若考慮到移除多餘的或不需要的控制（ 特別是若該控制有高維護成本 ），宜將資訊安全和成本因素納入考量。因為控制可能相互影響，移除多餘的控制可能降低目前整體的安全。此外，將多餘或不需要的控制留在原處可能比移除更為便宜。

風險處理選項宜將下列各項納入考量：

- 受影響的各方如何感知風險
- 溝通至各方的最適方式

全景建立(參見7.1 - 風險評估準則 ）提供組織需要遵循的法律和法規要求資訊。宜施行限定未能遵循和處理選項對組織之風險的可能性。在風險處理時宜考量在全景建立活動期間識別出之組織、技術、結構等的所有限制。

一旦定義了風險處理計畫，則需決定剩餘風險。考量所提出風險處理的預期效果後。此事涉及風險評鑑的更新或再循環。萬一剩餘風險仍未能滿足組織的風險接受準則，在繼續進行風險接受前，可能需要更進一步的風險處理循環。

ISO/IEC27002 (CNS 27002 ）的0.3節內有更多資訊。

產出：受限於組織管理者的接受決策之風險處理計畫和剩餘風險。

風險處理-降低

行動：宜經由選擇控制項減低風險等級，使剩餘風險得被重新評鑑至可接受的風險。

實作指引：

宜選擇合適與正當的控制措施，以符合風險評鑑和風險處理所識別出的要求。該選擇宜考量風險接受準則與法律、法規和契約的要求，該選擇亦宜考量控制措施施行的成本與時間範圍，或技術、環境與文化層面。適當地選擇資訊安全控制項通常可能降低總擁有成本。

一般而言，控制措施可能提供下列的一種或多種保護：矯正、排除、預防、衝擊最小化、制止、偵測、復原、監控與認知。在控制措施的選擇中，權衡控制措施購置、施行、管理、營運、監控和維護成本，以及被保護資產的價值。再者，宜考慮某些控制措施就風險減低和利用新業務機會之潛力而言的投資回報。此外，宜考慮可以不需要去定義與施行新控制措施或修改現有控制措施的專業技巧。

ISO/IEC 27002 (CNS 27002 ）提供控制項的詳細資訊。

有許多會影響控制措施選擇的限制。技術上的限制如執行績效的要求、可管理性（ 營運的支援要求 ）與相容性議題可能阻礙某些控制措施的使用或可能導致人為錯誤，不是抵銷了控制、產生不正確的安全感或甚至增加大於沒有該控制措施的風險（ 如要求複雜的通行碼而無適當的訓練，導致使用者寫下通行碼 ）。而且，也有單一控制措施會影響執行績效的案例。管理者宜嘗試去識別在保證充分的資訊安全時能滿足執行績效要求的解決方案。本步驟的結果是帶有成本、利益和施行優先順序之可能控制措施的清單。

在選擇控制措施和施行時宜考量不同的限制。一般而言，要考慮下列項目

- 時間限制
- 技術限制
- 文化限制
- 環境限制
- 容易使用
- 整合新的和現有控制措施的限制
- 財務限制
- 營運限制
- 道德倫理限制
- 法律限制
- 人員限制

風險處理-接受

行動：宜依據風險評估採用保留風險而不進一步行動的決策。

註 ISO/IEC 27001 (CNS 27001) (第4.2.1 (f) (2) 節) “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”描述相同的活動。

實作指引：

若風險等級滿足風險接受準則，則不需要施行額外的控制，且得保留該風險。

風險處理-避免

行動：宜避免增加特定風險的活動或情況。

實作指引：

當已識別的風險被認為太高時，或施行其它風險處理選項的成本超過利益時，可作出完全避免風險的決定，籍由從已規劃或現有活動或一組活動中退出，或變更活動運作的情況。舉例而言，對本質所引起的風險，最有成本效益的替代方案就是將該資訊處理設施實體地搬移到風險不存在或是在控制下的地點。

風險處理-轉移

行動：宜將風險轉移到依據風險評估最能有效管理該特定風險的另一方。

實作指引：

風險轉移牽涉到與外部團體分享某些風險的決策。風險轉移得產生新的風險或修改現有、已識別的風險。因此，可能需要額外的風險處理。

轉移可藉由將支援後果的保險，或藉由轉包給監控資訊系統並在造成已定義的損害等級前採取立即行動以阻止攻擊角色的合夥人來完成。

宜注意的是可能可以轉移管理風險的職責，但正常地不可能轉移衝擊地責任。客戶通常將不利衝擊歸因於組織的錯誤。

課程大綱

- 資訊安全風險評鑑
- 資訊安全風險處理
- 資訊安全風險接受
- 資訊安全風險溝通
- 資訊安全風險監控與審查

資訊安全風險接受

投入：受限於組織管理者接受決策的風險處理計畫和剩餘風險評鑑。

行動：宜作接受該決策的風險和職責的決策並正式地記錄（ 與ISO/IEC 27001 (CNS 27001）第4.2.1(h）節有關 ）。

實作指引：

風險處理計畫宜描述如何處理已評鑑的風險以滿足風險接受準則（ 參見7.2節風險接受準則 ）。審查和核准所提出的風險處理計畫和所導致的剩餘風險，並且記錄該核准有關的情況，對負責任的管理者而言是重要的。

風險接受準則可能比只決定剩餘風險是否落於單一定限之上或下更為複雜。多數案例中，剩餘風險的等級可能無法滿足風險接受準則，因為伴隨風險的利益是非常有吸引力的，或因為風險減低的成本太高。此情勢顯示風險接受準則不足，且若可能宜加以修訂。然而，並不總是可以即時地修訂風險接受準則。在該案例中，決策者可能必須接受不滿足正常接受準則的風險。若此為必要，決策者宜明白地在該風險上註解並包含一決策的正當理由，以推翻正常的風險接受準則。

產出：對不能滿足組織正常風險接受準則的風險有正當理由的已接受之風險清單。

課程大綱

- 資訊安全風險評鑑
- 資訊安全風險處理
- 資訊安全風險接受
- 資訊安全風險溝通
- 資訊安全風險監控與審查

資訊安全風險溝通

風險溝通是決策者與其他事件相關者藉由交換分享風險資訊就如何管理風險達成協議的活動。資訊包括，但不限於下列，風險的本質、形式、可能性、嚴重性，處理與接受度。

由於對必須作的決策可能有重大的衝擊，事件相關者間有效的溝通是重要的。溝通將確保負責施行風險管理的人和既得利益者了解決策的基礎以及為何需要特定的行動。溝通是雙向的。

在與風險有關或在討論議題時，事件相關者由於假設、觀念和需求、議題和關切等的差異，對風險的認知可能不同。事件相關者似乎會基於其對風險的認知而對風險的可接受性作判斷。識別與記錄以及清楚地了解根本理由並處理，對於要確保事件相關者對風險的認知及對利益的認知，是特別重要的。

宜執行風險溝通以達下列目的：

- 提供組織風險管理結果的確保
- 收集風險資訊
- 分享來自風險評鑑的結果並提出風險處理計畫
- 避免或降低因決策者和事件相關者間缺乏互相了解而導致資訊安全危害的發生與後果
- 支援作決策
- 取得新的資訊安全知識
- 與他方協調並規劃降低任何事故後果的回應
- 給予決策者與事件相關者對風險的責任感
- 改善認知

組織宜發展正常營運與緊急情況下的風險溝通計畫。因此，風險溝通活動宜是持續執行的。

主要決策者與事件相關者間的協調可藉由委員會的成立而達到，委員會內可舉行有關風險、優先順序及適當處理、接受等的辯論。

在組織內與適切的公共關係或溝通單位合作以協調所有與風險溝通有關的任務是重要的。在如回應特定的事故的危機行動事故中，是決定性的。

產出：對組織的資訊安全風險管理過程和結果持續的了解。

課程大綱

- 資訊安全風險評鑑
- 資訊安全風險處理
- 資訊安全風險接受
- 資訊安全風險溝通
- 資訊安全風險監控與審查

資訊安全風險監控與審查-風險因素的監控和審查

風險不是靜態的。威脅、脆弱性、可能性或後果可無徵兆的突然變更。 所以不停的監控是必要的以偵測這些變更。也可由提供有關新威脅或脆弱性資訊的外部服務來支援。

組織宜確保持續監控下列項目：

- 被包含在風險管理範圍內的新資產
- 必要的資產價值修改，如由於改變的業務要求
- 組織外部與內部可能生效的、未被評鑑過的新威脅
- 新的或增加的脆弱性可能允許威脅利用這些新的或增加的脆弱性之可能性
- 決定已經曝露於新的或再出現的威脅的已識別之脆弱性
- 已評估過的威脅、脆弱性和風險經集合可導致無法接受等級的風險的衝擊或後果
- 資訊安全事故

新威脅、脆弱性或可能性變更或後果可增加之前評估為低風險的風險。對低和可接受風險的審查宜對每一風險分別考量，也要將所有該類風險集合在一起考量，以評估它們的潛在累積衝擊。若風險未落入低或可接受風險類，宜使用第 9 節的一項或更多項目處理。

影響威脅發生之可能性和後果的因素，和影響各種處理選項之適當性或成本的因素均可能變更。影響組織的重要變更宜是更特定審查的理由。因此，風險監控活動宜定期地重覆，且所選擇的風險處理選項宜週期性地審查。

風險監控活動的結果可投入其它的風險審查活動。組織宜定期審查所有的風險，發生重要變更時亦同（ 依據 ISO/IEC 27001 (CNS 27001）第4.2.3節 ）。

產出：風險管理與組織業務目標、風險接受準則的持續性調校一致。

資訊安全風險監控與審查-風險管理監控、審查與改善

持續地監控和審查以確保風險評鑑和風險處理的全景、結果，以及管理計畫、保持情勢的相關與適切是必要的。

組織宜確保資訊安全風險管理過程和相關活動在現今與其後的情勢保持為適切的，任何對改善過程遵循所協議的過程或行動改善宜對適當的管理者予以識別造以確保未忽略或低估風險或風險元件。且採取必要的行動與作決策，以提供實際的風險了解和回應能力。

此外，組織宜定期驗證用來量測風險與其元件的準則仍然有效並與業務目標、策略和政策一致，同時業務全景的變更在資訊安全風險管理過程中要充分地納入考量。此監控和審查活動宜處理（但不限於）：

- 法律和環境背景
- 競爭背景
- 風險評鑑方法
- 資產價值和種類
- 衝擊準則
- 風險評估準則
- 風險接受準則
- 總擁有成本
- 必要資源

組織宜確保風險評鑑和風險處理資源在審查風險、處理新或變更的威脅或脆弱性上持續地可用，以及據此建議管理階層。

風險管理監控能導致修改或增加所使用的方法取徑（Approach）、方法論或工具，依據：

- 識別的變更
- 風險評鑑循環
- 資訊安全風險管理過程所描準的方向（如業務持續性、對事故的彈性、遵循性）
- 資訊安全風險管理過程的目標（如組織、業務單位、資訊處理、其技術施行、應用系統、與網際網路的連結）

產出：資訊安全風險管理過程對組織業務目標的持續關聯或修改過程。

簡報完畢，敬請指教！

吳昭儀

joycewu@nii.org.tw

NII產業發展協進會