教育體系資通安全暨個資管理制度說明

財團法人中華民國國家資訊基本建設產業發展協進會

NII 產業發展協進會
☏ (02) 2508-2353
✉台北市松江路 317 號 7 樓

簡報大綱

1. 緣起
2. 本文框架差異
3. 教育體系資通安全暨個資管理制度說明
4. 附錄A 資通安全管理規範

緣起

緣起

- 資通訊科技的快速發展，對於作業效率之提供有所助益，惟其亦帶來了資通安全之挑戰。為能夠有效因應資通訊科技應用所帶來的資通安全挑戰，教育部(以下稱本部)於民國(以下同)96年5月30日發布「教育體系資通安全管理規範」，供教育體系機關(構)與各級學校據以建立其資通安全管理系統，綜合考量其重要性、急迫性以及可分配資源等因素，建立其資通安全管理規範的設計與施測，透過持續改善的管理機制運行，大幅強化其資通安全的有效性。

緣起

- 「教育體系資通安全管理規範」自施行迄今已逾九年，其間經歷資通訊環境之變遷，諸如：網路之普及、資通訊科技之進步與廣泛應用、資通訊安全最佳實務標準於102年改版、以及組織架構與運作模式轉變等，有必要重新檢視與調整。復以我國於99年將電腦個人資料保護法修改為個人資料保護法，擴大保護標的，不限於經電腦處理之個人資料，且以任何形式存在之個人資料皆有該法之適用。其次則是擴大適用範圍，舉凡涉及個人資料蒐集、處理、利用之個人、法人或團體皆為該法之適用，且各行各業皆應適用該法。第三，新增個人資料蒐集、處理與利用之行為規範，諸如：告知義務之履行，並提高損害賠償之額度且導入團體訴訟之機制。此外，我國於104年針對99年修正之個人資料保護法，因應實務運作之需求，完成第二次修法，包括：將病歷納入特種個人資料之範圍，新增當事人書面同意為特種個人資料之蒐集、處理與利用依據等。前揭法令之更迭對於教育體系造成相當程度之影響，且教育體系發生個人資料遭不當揭露或利用之情況亦曾見聞。是以，於維護資通安全之際，尤有必要考量個人資料安全之維護。

緣起

- 爰此，為因應資通訊環境之變化，並考量我國個人資料保護法之修正與施行，以及最佳國際實務標準之發展與普及，如ISO 27001:2013、ISO 27002:2013、ISO 29100:2011、BS 10012:2009等，自104年起著手「教育體系資通安全管理規範」之研修，歷經數次之專家討論與教育體系意見諮詢，終而於105年完成之修訂，提出新版之「教育體系資通安全暨個人資料管理規範」。(以下稱本規範)

簡報大綱

1. 緣起
2. 本文框架差異
3. 教育體系資通安全暨個資管理制度說明
4. 附錄A 資通安全管理規範

本文框架差異

教育體系資通安全管理規範

- 壹、緣起
- 貳、簡介
- 參、適用範圍
- 肆、目標期程
- 伍、引用標準
- 陸、關於適用性聲明(Statement of Applicability)
- 柒、用詞解釋
- 捌、關於資訊安全管理系統(ISMS)建置步驟
- 玖、關於資訊安全管理系統(ISMS)建置需求

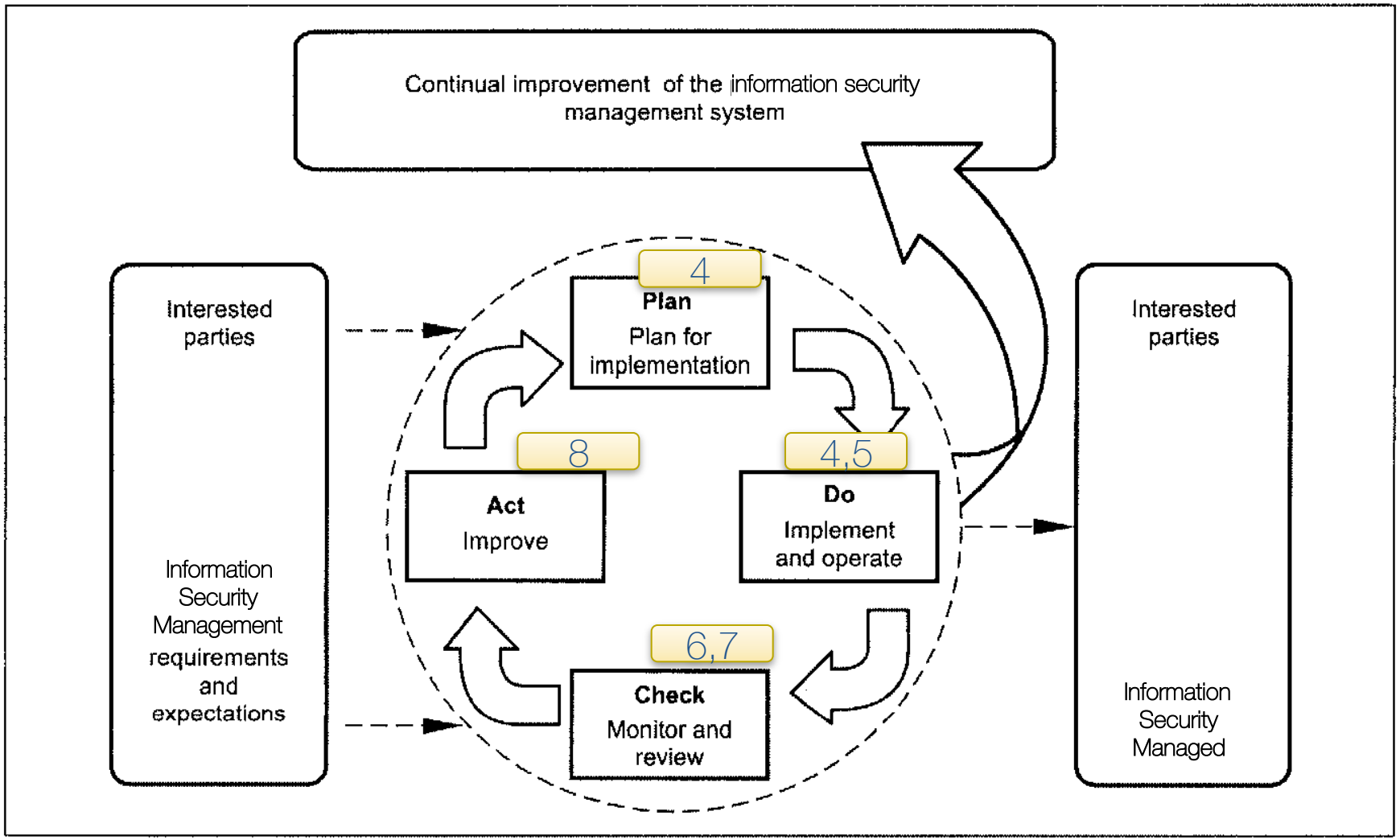
教育體系資通安全暨個人資料管理規範

- 壹、緣起
- 貳、簡介
- 參、適用範圍
- 肆、目標期程
- 伍、引用標準
- 陸、適用性聲明（Statement of Applicability）
- 柒、建置步驟及需求

本文

舊版	新版
壹、 緣起	壹、緣起
貳、 簡介	貳、簡介
參、 適用範圍	參、適用範圍
肆、 目標期程	肆、目標期程
伍、 引用標準	伍、引用標準
陸、 關於適用性聲明(Statement of Applicability)	陸、適用性聲明（Statement of Applicability）
柒、 用詞解釋	
捌、 關於資訊安全管理系統(ISMS)建置步驟	柒、建置步驟及需求
玖、 關於資訊安全管理系統(ISMS)建置需求	

ISO 27001:2005 (PDCA) cycle



教育體系資通安全管理規範

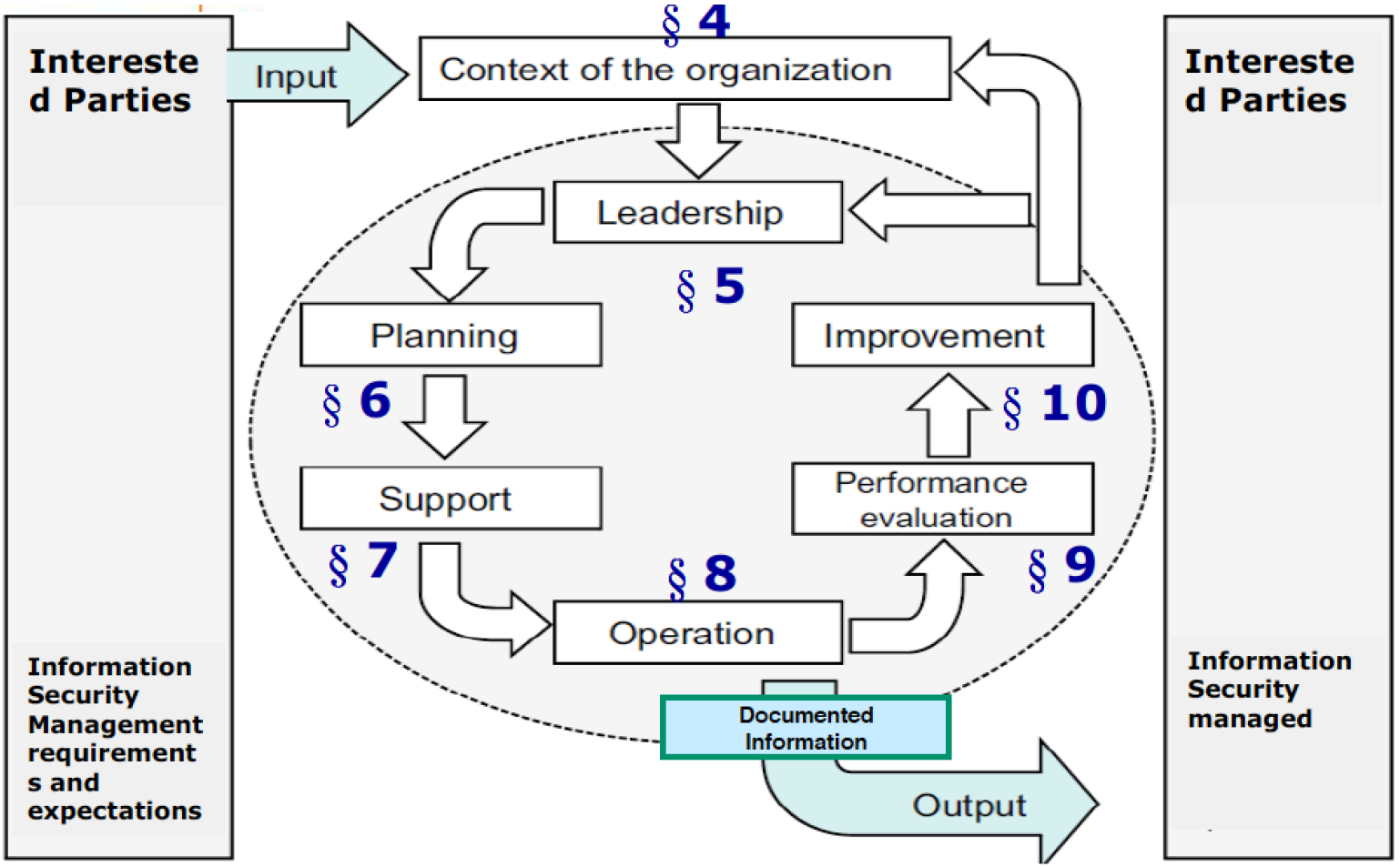
捌、關於資訊安全管理系統(ISMS)建置步驟

捌、三 ISMS之建立	捌、四 ISMS之實施與操作	捌、五 ISMS之監控與審查	捌、六 ISMS之維持與改進

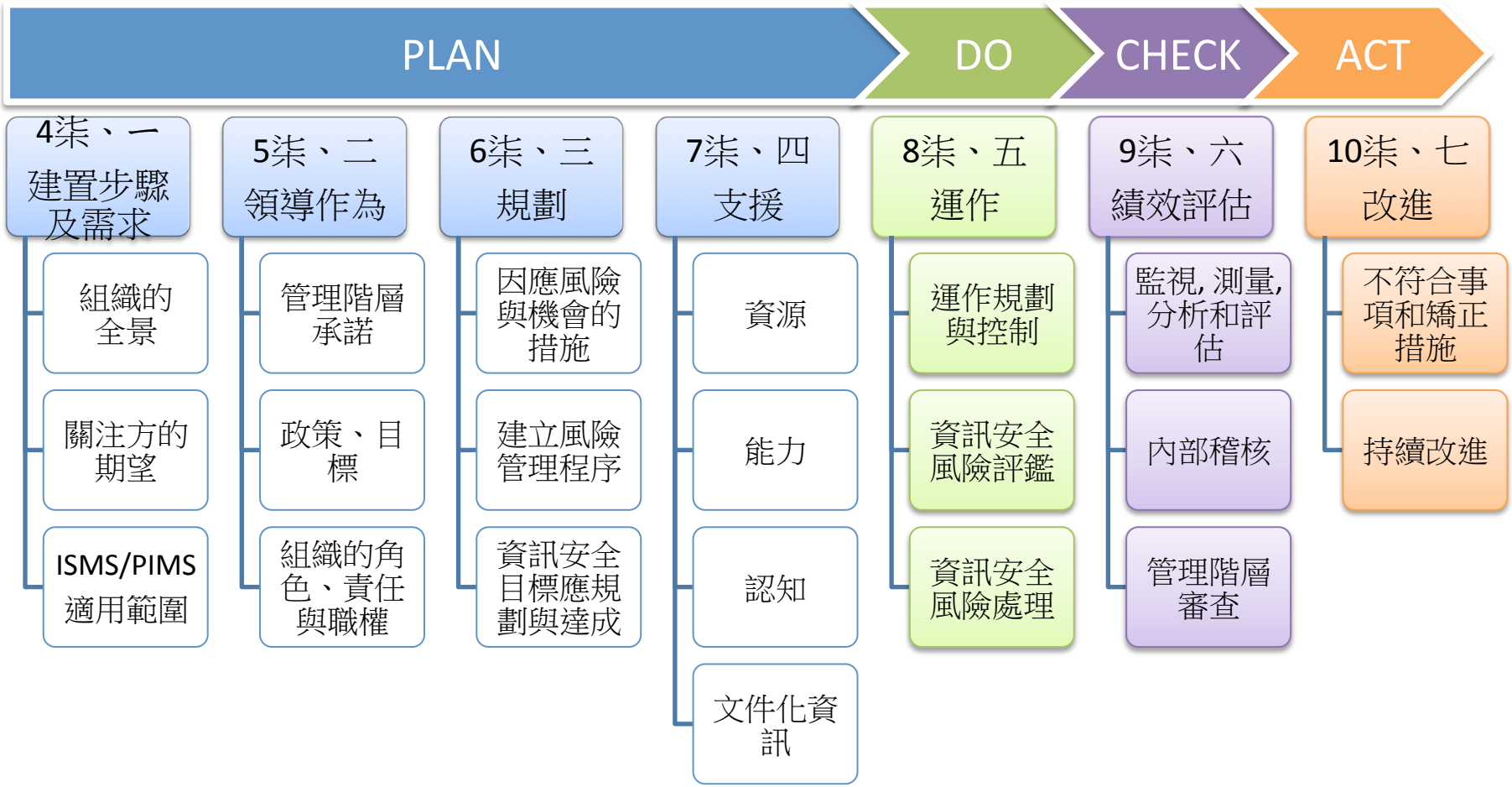
玖、關於資訊安全管理系統(ISMS)建置需求

玖、七 文件化要求	玖、八 管理階層責任	玖、九 管理階層審查	玖、十 ISMS之改進

採用ISO Annex SL之高階架構



教育體系資通安全暨個人資料管理規範新版框架



附錄及參考資訊

- 附錄A 資通安全管理規範
- 附錄B 個人資料管理規範
- 附錄C 個人資料保護規範對照表
- 附錄D 規範詞彙與定義
- 參考附錄 隱私強化技術
- 資通安全管理規範實施自評表
- 個人資料管理規範實施自評表
- 參考文件一-教育部與所屬機關(構)及學校資通安全責任等級分級作業規定.pdf
- 參考文件二-資訊系統分級與資安防護基準作業規定
- 參考文件三-政府機關(構)資安事件數位證據保全標準作業程序

適用範圍

舊版

- 第一群（大專以上）：
  - 本群適用單位以教育部電算中心、部屬館所、縣市網中心、公私立大專院校（計網中心及校務行政）等為主。
- 第二群（高中職）：
  - 本群適用範圍以高中職學校（資訊管理單位或因規模、資源因素轉至本群者及校務行政）為主要對象。

- 新版
- A級：
  - ISMS：應至少包含組織內所有資訊管理作業與流程，全部核心業務應用資訊系統與網路系統，以及受委託執行國家安全與機密資訊或技術研究單位，或試務管理單位。
  - PIMS：應包含組織內全部所有涉及個人資料蒐集、處理與利用之流程。
- B級：
  - ISMS：應至少包含資訊管理單位、學術網路系統、核心業務資訊系統。
    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。
- C級：
  - ISMS：應至少包含資訊管理單位及校務行政資訊系統。
    PIMS：應至少包含組織內涉及個人資料處理蒐集、處理與利用流程之行政單位，以及資訊管理單位。

各級教育機構適用控制項對照表

- 第一學群之控制措施(計101項)
- 第二學群之控制措施(計69項)

- A級單位建議納入所有控制措施(計114項)
- B級單位採用(計101項)
- C級單位使用 (計51項)

簡報大綱

1. 緣起
2. 本文框架差異
3. 教育體系資通安全暨個資管理制度說明
4. 附錄A 資通安全管理規範

教育體系資通安全暨個人資料管理規範2016年版修正說明

簡介

- 本規範因應個人資料保護法之修正與施行，新增個人資料管理系統（Personal Information Management System，以下稱PIMS）之相關要求，期以PDCA (Plan-Do-Check-Act，規劃-實行-確認-行動)策略，協助教育體系機關(構)與各級學校完善其個人資料安全維護之工作，達到個人資料保護之目的，降低個人資料遭不當揭露或利用之風險。同時，本規範因應最佳實務標準102年之改版，新增資訊安全管理系統（Information Security Management System，以下稱ISMS）之相關控制措施建議，期能夠協助教育體系機關(構)與各級學校有因應資通訊科技應用所衍生之新興資通安全議題。此外，為達資源有效運用之目的，本規範特別針對結合ISMS與PIMS之「資通安全暨個人資料管理系統」進行說明，期能夠協助教育體系機關(構)與各級學校評估其組織規模、管理需求、目標、結果等因素，建置能夠同時符合資通安全維護與個人資料保護目標之管理系統。

簡介

- 本規範期望對教育體系機關(構)與各級學校之資通安全或個人資料管理產生引導作用，協助其有效率地建置與運行資通安全與個人資料管理系統，發揮「事前預防·事後抑制」之效果，有效落實個人資料保護法令之施行，並達維護資通安全之目的。是以，教育體系機關(構)與各級學校於參照本規範建立管理系統時，得衡酌組織規模、業務特性、所欲達成之資通安全維護或個人資料保護目的等因素，選擇適當之實施範圍，配置適當之資源與人員，規劃適宜之管理系統，持續有效地運行該系統，並定期檢視與改善該系統。然而，值得注意是個人資料保護法令之遵循係屬全組織應遵循之事宜，且資通安全之風險非僅肇因於系統風險，故教育體系機關(構)與各級學校宜逐步擴大實施範圍，以達維護資通安全與個人資料保護之目的。

簡介

- 除本規範另有規定，選擇單獨建置ISMS之單位，無須執行關於PIMS之要求，反之亦然；選擇建立「資通安全暨個人資料管理系統」，應同時符合二項管理系統之要求。意即，教育體系機關(構)與各級學校得就ISMS或PIMS擇一驗證，亦可就ISMS與PIMS同時驗證。然而，本規範之驗證作業目的係為協助導入機關(構)與學校確認其所建置資通安全或個人資料管理系統之有效性，如有發生個人資料保護之爭議，仍應依個案為具體判斷，非謂經驗證通過即可謂無法律責任。

適用範圍

- 本規範適用於教育體系機關(構)與各級學校，其得參照本規範所訂之管理要求與執行方法，針對資通安全與(或)個人資料安全之維護建立管理系統，就組織規模、業務特性等選擇適當之實施範圍，配置適當之資源與人員，規劃適宜之管理系統，持續有效地運行該系統，並定期檢視與改善該系統。
- 有鑑於教育體系機關(構)與各級學校之層級、組織規模、業務特性差異極大，為避免其因組織特性無法執行部分要求，本規範爰參考行政院國家資通安全會報訂定之「政府機關（構）資通安全責任等級分級作業規定」與教育部頒定之「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」，將適用機關(構)及學校分為A、B、C三級(各級涵蓋之對象請參閱教育部與所屬機關(構)及學校資通安全責任等級分級作業規定)，並依等級建議不同之適用範圍，如下：

適用範圍

- A級：
- ISMS：應至少包含組織內所有資訊管理作業與流程，全部核心業務應用資訊系統與網路系統，以及受委託執行國家安全與機密資訊或技術研究單位，或試務管理單位。
- PIMS：應包含組織內全部所有涉及個人資料蒐集、處理與利用之流程。
  - B級：
- ISMS：應至少包含資訊管理單位、學術網路系統、核心業務資訊系統。
  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。
  - C級：
- ISMS：應至少包含資訊管理單位及校務行政資訊系統。
  PIMS：應至少包含組織內涉及個人資料處理蒐集、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。

目標期程

- 本規範之目標，係提供所有教育體系機關(構)與學校，考量自身資源及所對應之風險，並依其適用範圍建置適合與有效之資通安全或個人資料管理系統，進而建立整合的「資通安全暨個人資料管理系統」。
- 管理系統之建立、實作、維持及持續改善，需考量管理階層的支持、各單位的協調配合、人力、經費等各項資源因素，因此，建議各單位採階段式進行建置，自行設定合理的期程目標，逐步達成每年度預定的進程比例，藉由如此的模式，最終能建置合適、整合的「資通安全暨個人資料管理系統」。

引用標準

- 本文架構主要採用ISO組織定義之 Annex SL架構，條文內容則同時參考ISO/IEC 27001:2013及BS 10012:2009兩項管理標準，再依據教育體系機關(構)與學校的特性及需求，設計出較為合適的規範，希冀能有效提升各機關(構)與學校的資通安全及個人資料管理能力。參考文件如下：
  - 個人資料保護法及個人資料保護法施行細則(法務部)
  - 私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法(教育部)
  - 行政院及所屬各機關資訊安全管理規範(行政院)
  - 政府機關（構）資通安全責任等級分級作業規定(行政院資通安全辦公室)
  - 教育體系機關構及學校資通安全責任等級分級作業規定(教育部)
  - 資訊系統分級與資安防護基準作業規定(行政院國家資通安全辦公室)
  - 政府機關構資安事件數位證據保全標準作業程序(行政院國家資通安全辦公室)
  - 教育體系個人資料安全保護基本措施(教育部)
  - 103年資安服務暨專案管理辦公室 安全控制措施參考指引（V2.0）

引用標準

- 本文架構主要採用ISO組織定義之 Annex SL架構，條文內容則同時參考ISO/IEC 27001:2013及BS 10012:2009兩項管理標準，再依據教育體系機關(構)與學校的特性及需求，設計出較為合適的規範，希冀能有效提升各機關(構)與學校的資通安全及個人資料管理能力。參考文件如下：
  - ISO/IEC 27001:2013 Information security management systems - Requirements。
  - ISO/IEC 27002:2013 Code of practice for information security controls。
  - BS 10012:2009 Data Protection Specification for a Personal Information Management System。
  - ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework。
  - ISO/IEC 29101:2013 Information technology – Security techniques – Privacy architecture framework。
  - ISO29191:2012 Information technology – Security techniques – Requirements for partially anonymous, partially unlinkable authentication

適用性聲明（Statement of Applicability）

- 本規範適用於教育體系機關(構)與學校，其得考量各自分級屬性、類型、規模、資源、業務性質、以及組織內部有關ISMS與PIMS之施行狀況，選擇控制措施並產生相關之適用性聲明。
- 一、有關ISMS之建置與施行
  - 擬建置ISMS之教育體系機關(構)與學校可依據前揭所提及之適用等級選擇控制措施，參考附錄A之控制措施，提出「ISMS適用性聲明」。各等級機關(構)與學校適用之控制措施請參照「附錄A 資訊安全管理規範 附件1各級教育機構適用控制項對照表」。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，且排除後不影響該機關(構)與學校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「資訊系統分級與資安防護基準作業規定」，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、開發及維護與A.15供應者關係等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（Statement of Applicability）

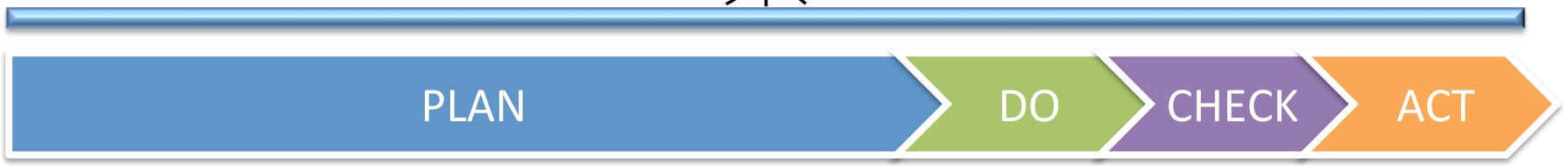
- 核心業務資訊系統：指經資訊系統分級後，等級為「高」者，資訊系統安全等級經鑑別為高者，則需進行風險評鑑以分析規劃實作控制措施之有效性。實際執行時，核心業務資訊系統或其他安全等級為高者，應依據適用安全等級高項目執行控制措施，其他中低安全等級系統，則僅依其等級選用控制措施即可。

- 二、有關PIMS之建置與施行
  - 建立並運行PIMS之機關(構)與學校，應選用附錄B所有控制項。
- 三、有關資通安全暨個人資料管理系統之建置與施行
  - 建立並運行整合的「資通安全暨個人資料管理系統」之機關(構)與學校，應同時遵循上述要求，並提出「資通安全暨個人資料管理系統適用性聲明」。

柒、建置步驟及需求

- 教育體系機關(構)與學校於建立、實作、維持及持續改善ISMS、PIMS或資通安全暨個人資料管理系統時，執行步驟及相關需求事項如下：
- 一、組織全景
  - 施行機關(構)或學校應依據相關法令要求、行政院及教育主管機關所下達之重要決定或指導(包括但不限於主管機關之行政指導、重要會議決議事項等)、組織透過相關會議所做成之決議(包括但不限於主管會報、行政會議或校務會議等之決)，針對資通安全或個人資料安全之維護需求進行評估，並據此建立或調整資通安全與個人資料管理範圍與目標。
  - 施行機關(構)或學校應依據決議事項確認其關注方(利害相關團體)與要求事項，並留存文件化紀錄。
  - 上述事項之識別與分析應定期審查(每年至少一次)，或於施行機關(構)或學校遭遇重大變更、或有新增業務時重新檢視，並供管理審查時，評估管理系統及其適用範圍是否有調整之必要性。

教育體系資通安全管理規範 新版框架



柒、一
建置步驟及需求

- 組織的全景
- 關注方的期望
- ISMS/PIMS 適用範圍

柒、二 領導作為

- （一）、領導及承諾
  - 管理制度管理人或召集人應由施行機關(構)或學校之副首長以上擔任或指定，並藉由下列事項，展現對管理制度之領導與承諾：
  - 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。
- （二）、建立政策與目標
  - 管理人或召集人應確保建立文件化的管理政策，並於機關(構)或學校內進行公告或傳達，同時依需要提供予利害相關團體。
  - 管理政策應包含符合機關(構)或學校之管理目的與目標、滿足管理制度要求事項與、以及持續改善之承諾。
  - 施行機關(構)或學校應依規劃期間或重大變更時，於透過管理審查管理活動評估管理政策與目標，並配合變更需求修訂政策與目標。

柒、二 領導作為

- （三）、指派角色、責任及權限
  - 管理人或召集人應建立制度管理小組，依機關(構)或學校特性，指派人員並賦予其管理之責任與權限，以促進達成本規範之要求事項。受指派人員應定期（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。ISMS與PIMS所配置人員應依據附錄A.6 資訊安全組織與附錄B.2 個人資料管理組織派任。

教育體系資通安全管理規範 新版框架

- 柒、一 建置步驟及需求
  - 組織的全景
  - 關注方的期望
  - ISMS/PIMS適用範圍
- 柒、二 領導作為
  - 管理階層承諾
  - 政策、目標
  - 組織的角色、責任與職權

柒、三 規劃

- （一）、管理目標達成風險與機會之因應行動
  - 為確保達成制度管理目標，並預防或減少非預期之影響，以達成持續改善，應依規劃期間或重大變更時，評估管理目標異動與達成情形，如有異動或未達成狀況，則應規劃因應風險與機會之行動，將各項行動整合及實作於管理制度中，並評估此行動之有效性。
  - PIMS並應依附錄B.4個人資料之識別與風險管理要求執行。
-
- （二）、建立風險管理程序
  - 應參考「資訊系統分級與資安防護基準作業規定」，鑑別適用範圍內資訊系統之安全等級。資訊系統經鑑別後，其安全等級屬最高等級者，應執行風險評估、擬訂與執行風險管理措施；其安全等級非屬最高等級者，應衡酌其風險程度，以決定是否進行風險評估、擬訂與執行風險管理措施。

柒、三 規劃

- 風險評估與管理流程建立應符合下列要求事項：
  - 建立與維持風險準則

    包含風險評鑑執行時機與方法，以及風險接受準則，以確保重複之風險評鑑能產生一致、有效及可比較之結果。
  - 識別、分析並評估風險

    識別管理制度適用範圍內涉及資訊之機密性、完整性、可用性與適法性相關聯之風險與風險擁有者。

    所識別之風險可能導致之潛在後果與發生的實際可能性，並將所建立之風險準則與風險分析結果進行比較，訂定風險處理優先順序。
  - 選擇風險處理措施

    考量風險評鑑結果，選擇適切之風險處理選項，並依選項決定所有必須實作之控制措施。
  - 產生或評估適用性聲明書(資訊安全風險處理使用)

    執行資訊安全風險評鑑時，應依據資訊資產分級結果重現檢視比較現有控制措施及附錄A，確認未忽略必要之控制措施，並產生或評估適用性聲明書，包括附錄A之控制措施，且不論是否實作，提供納入或排除之理由。
  - 制訂風險處理計畫並取得核准

    制訂風險處理計畫，並取得風險擁有者對風險處理計畫之核准，以及對剩餘風險之接受。

柒、三 規劃

- （三）、管理目標及其達成之規劃
  - 施行機關(構)或學校應針對異動與未達成之管理目標，設定符合管理政策與策略之可量測指標，並保存管理目標之文件化資訊。
  - 施行機關(構)或學校應對前述管理目標規劃因應行動，包含：
    - 相關執行活動或事項。
    - 所需配置之人員、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。

教育體系資通安全管理規範 新版框架

柒、四 支援

- （一）、資源
  - 施行機關(構)或學校應依據管理目標達成規劃，提供建立、實行、維持及持續改善管理制度所需資源。
- （二）、能力
  - 施行機關(構)或學校應採取下列措施：
    - 指派受過適當教育訓練、具備證照或具有經驗人員，執行資通安全或個人資料管理相關任務；規劃培訓以強化人員能力時，應評估培訓之有效性。
    - 有關人員能力訓練，ISMS應參照附錄A .7人力資源安全，PIMS則依附錄B.3 人員認知與訓練要求執行。
    - 應保存文件化資訊(如：如證書、證照、培訓紀錄等)，作為人員勝任之證據。
- （三）、認知
  - 應規劃人員認知宣導或訓練，讓所有人員知悉：
    - 管理政策及目標。
    - 管理程序與流程，要求事項與人員責任。
    - 未遵循要求可能產生對個人與單位的影響與衝擊，包含但不限於獎懲措施。
  - ISMS應參照附錄A .7人力資源安全，PIMS則依附錄B.3 人員認知與訓練要求執行。

柒、四 支援

- （四）、文件化資訊
  - 管理制度文件化資訊應滿足下列要求：
  - 管理制度文件應包括本規範要求之文件化資訊，及施行機關(構)或學校要求管理制度為達成其有效性之文件化資訊與作業紀錄。
  - 其文件化資訊至少應包含：
    - 決議事項確認其關注方(利害相關團體)與要求事項
    - 管理政策
    - 管理目標
    - 人員勝任之證據
    - 管理制度執行證據
    - 風險處理計畫與風險處理結果
    - 有效性評估證據
    - 管理審查執行之證據
    - 不符合項目及矯正措施
    - 制訂及更新應遵循既有文件管理程序，進行審查及核准。
    - 管控文件化資訊派送、存取、檢索、使用、儲放與維護、變更管制、留存及屆期處置，並適切保護。
    - 施行機關(構)或學校應識別對管理制度規劃及運作必要之外部文件。

教育體系資通安全管理規範 新版框架

- 柒、一 建置步驟及需求
  - 組織的全景
  - 關注方的期望
  - ISMS/PIMS 適用範圍
- 柒、二 領導作為
  - 管理階層承諾
  - 政策、目標
  - 組織的角色、責任與職權
- 柒、三 規劃
  - 因應風險與機會的措施
  - 建立風險管理程序
  - 資訊安全目標應規劃與達成
- 柒、四 支援
  - 資源
  - 能力
  - 認知
  - 文件化資訊

柒、五 運作

- （一）、運作之規劃及控制
  - 施行機關(構)或學校之管理制度運作應滿足下列要求：
    - 應依據管理制度各階文件，以及為達成管理目標所規劃之流程、程序與控制措施執行，並應保存執行證據。
    - ISMS應依據所屬級別實作選定之附錄A控制措施，PIMS則應實作附錄B訂定之控制措施。
    - 應確保各項委外執行作業受到控制與管理，屬ISMS委外管理可連結附錄A 之A.15供應者關係，PIMS則依據附錄B之B.12委外管理執行。
- （二）、執行風險評鑑
  - 施行機關(構)或學校依規劃期間(至少每年一次)、管理階層指示或發生重大變更後一個月內，應執行風險評鑑，確認管理制度各項風險加以識別，並保存風險評鑑執行紀錄。
  - PIMS施行機關(構)或學校應分析可能造成當事人損失或困擾之個人資訊處理流程，由風險擁有者進行審查。
  - 擬定風險處理計畫，並取得風險擁有者對其及剩餘風險之核准。
- （三）、實作風險處理
  - 施行機關(構)或學校應實作風險處理計畫並保存風險處理結果之文件化證據資訊。

教育體系資通安全管理規範 新版框架

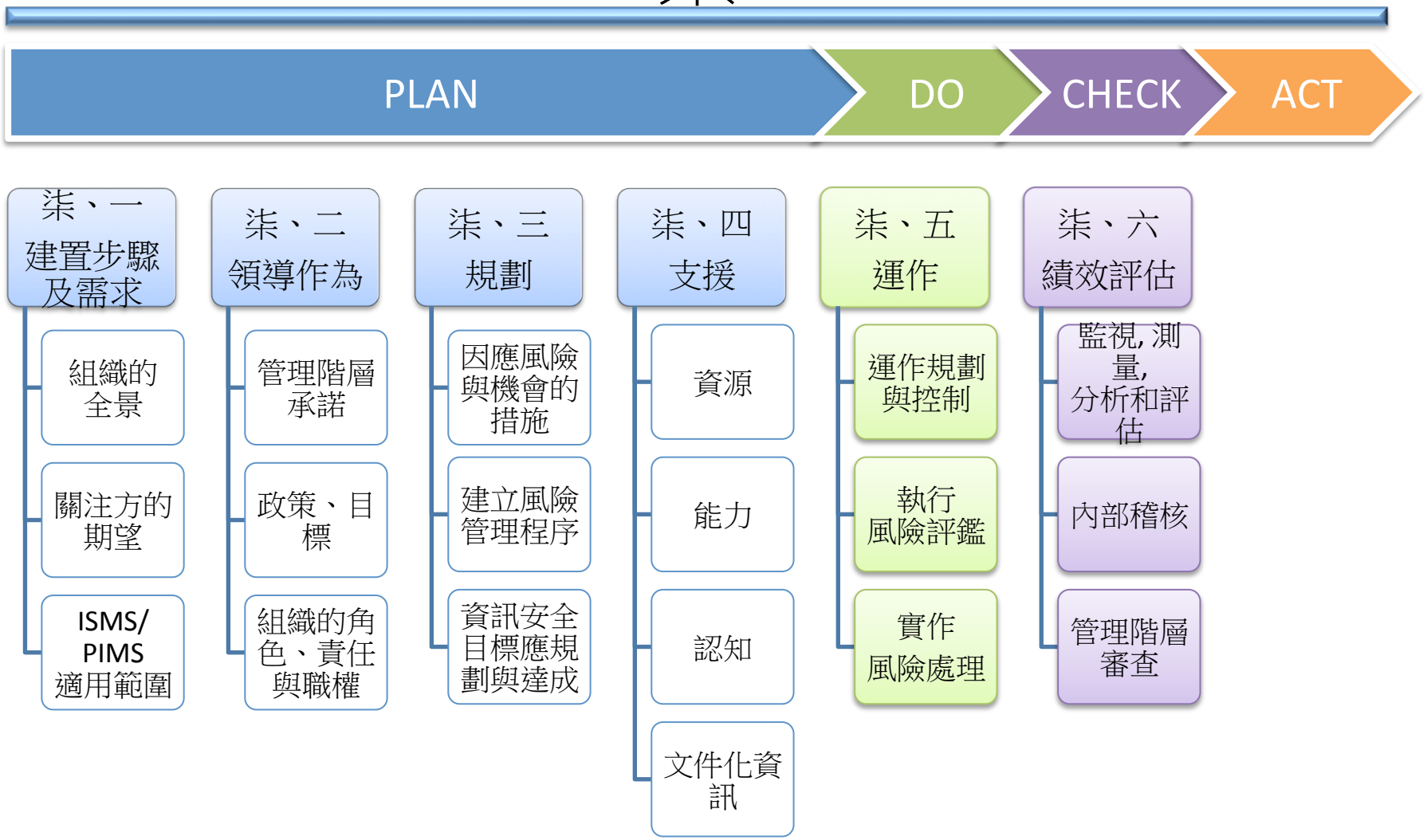
柒、六 績效評估

- 監督、量測、分析及評估
  - 施行機關(構)或學校應針對已施行之常態性作業流程或控制措施建立監督機制，如機房管理、網路管理作業審查等。
  - 對於該年度異動之管理目標，以及風險處理措施設定有效性量測指標，並界定明確計算方式與資料來源、量測人員、週期與時間點，以及分析及評估量測結果之人員、週期與時間點。
  - 應留存文件化資訊，作為有效性評估證據。
- 內部稽核
  - 施行機關(構)或學校應定期(至少每年一次)或於重大變更後執行一次內部稽核，以確認機關(構)或學校與人員是否遵循本規範與機關(構)或學校管理程序要求，並有效實作及維持管理制度。ISMS施行機關(構)或學校可連結附錄A.18遵循性執行。
  - 稽核程序應包括頻率、方法、職責、規劃要求事項及報告。稽核計畫應包含適用範圍內核心業務與高風險個人資料流程或系統，並將前次稽核之結果納入考量。
  - 稽核員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性。
  - 稽核結果應對相關管理階層報告，留存相關紀錄以作為稽核計畫及稽核結果之證據。

柒、六 績效評估

- 管理審查
  - 管理小組應定期(每年至少一次)進行管理審查，以審查管理制度執行狀況，並確保其持續的適切性、合宜性及有效性。
  - 管理審查應包含下列討論事項：
    - 過往管理審查之議案的處理狀態
    - 資通訊安全或個資管理要求的變更，如上級機關要求、最高行政管理會議決議事項
    - 管理目標與指標量測結果
    - 內外部稽核結果
    - 資安事故與不符合項目之矯正情形
    - 風險評鑑結果及風險處理計畫執行進度
    - 持續改善之機會
    - 管理審查決議事項應包含持續改善機會與管理制度變更需求之決議。
    - 施行機關(構)或學校應保存相關紀錄，以作為管理審查執行之證據。

教育體系資通安全管理規範 新版框架



改善

- 不符合項目及矯正措施
  - 不符合項目發生時，施行機關(構)或學校應進行下列作為，並保存紀錄：
  - 先對不符合項目採取行動以控制並矯正，進而處理其後果。
  - 判定其發生原因及矯正措施，並評估是否有其類似不符合項目存在，並據此提出並執行矯正措施，並必要時得考量對管理制度進行變更。
- 持續改善
  - 施行機關(構)或學校應持續改善管理制度的合宜性、適切性及有效性。

教育體系資通安全暨個人資料管理規範新版框架

- 4柒、一 建置步驟及需求
  - 組織的全景
  - 關注方的期望
  - ISMS/PIMS 適用範圍
- 5柒、二 領導作為
  - 管理階層承諾
  - 政策、目標
  - 組織的角色、責任與職權
- 6柒、三 規劃
  - 因應風險與機會的措施
  - 建立風險管理程序
  - 資訊安全目標應規劃與達成
- 7柒、四 支援
  - 資源
  - 能力
  - 認知
  - 文件化資訊
- 8柒、五 運作
  - 運作規劃與控制
  - 資訊安全風險評鑑
  - 資訊安全風險處理
- 9柒、六 績效評估
  - 監視, 測量, 分析和評估
  - 內部稽核
  - 管理階層審查
- 10柒、七 改進
  - 不符合事項和矯正措施
  - 持續改進

簡報大綱

1. 緣起
2. 本文框架差異
3. 教育體系資通安全暨個資管理制度說明
4. 附錄A 資通安全管理規範

教育體系資通安全暨個人資料管理規範2016年版附錄a修正說明

教育體系資通安全管理規範 附錄A

- 本標準列出之控制目標與控制措施乃參考 ISO/CNS 27001:2013附錄A控制措施，並依據原有「教育體系資通安全規範」，以及教育體系與相關單位既有之屬性與特點，歸納各等級應有安全控制措施。
- 為方便各施行單位承辦人員與驗證稽核人員參照國際與國家標準的要求與實作指引。本規範控制措施條文要求援引ISO/CNS 27001:2013附錄A控制措施的條文編號與說明，而控制措施實作指引中，屬原有控制措施者依據原有「教育體系資通安全規範」進行說明，新增控制措施部分則增加ISO/CNS 27002:2013 實作指引說明。各單位在實作時宜參考相關內容，以確保執行的完整性，實作指引說明將如有「應」一字為必要執行項目，「宜」一字則為可選擇是否執行之項目，施行單位可依據其資訊系統特性與風險狀況選用適當之實作方式。

教育體系資通安全管理規範 附錄A

- 同時，為減少各施行單位轉換上的困難，援引原有學群分類方式進行安全等級歸類。施行單位可依據「附件1各級教育機構適用控制項對照表」之建議導入各適用之控制措施，同時應參考「資訊系統分級與資安防護基準作業規定」，鑑別適用範圍內資訊系統之安全等級，施行單位識別出具有等級為「高」者之資訊系統時，則應加入A.14系統獲取、開發及維護與A.15供應者關係等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。各單位得考量自身之需求與特性，考慮增加其他必要之控制目標及控制措施。
-
- 附註：控制項編號下(I/P)註記代表ISMS與PIMS可共用項目，並以規範建置步驟與附錄A控制項編號進行對照，俾便施行單位進行ISMS的建置作業，同時導入PIMS則應考量適用該共用項目以符合ISMS與PIMS的要求。

附錄A 資通安全管理規範
控制目標概要

附錄A 控制目標與控制措施

舊版	新版
A.5 資訊安全政策訂定與評估	A.5 資訊安全政策訂定與評估
A.6 資訊安全組織	A.6 資訊安全組織
A.7 資訊資產分類與管制	A.7 人力資源安全
A.8 人員安全管理與教育訓練	A.8 資產管理
A.9 實體與環境安全	A.9 存取控制
A.10 通訊與作業安全管理	A.10 密碼學(加密控制)
A.11 存取控制安全	A.11 實體及環境安全
A.12 系統開發與維護之安全	A.12 運作安全
A.13 資訊安全事件之反應及處理	A.13 通訊安全
A.14 業務永續運作管理	A.14 系統獲取、開發及維護
A.15 相關法規與施行單位政策之符合性	A.15 供應者關係
	A.16 資訊安全事故管理
	A.17 營運持續管理之資訊安全層面
	A.18 遵循性

A.5 資訊安全政策訂定與評估

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.5 資訊安全政策					A.5
控制目標	A.5.1	資訊安全之管理指導方針		B.1.1	A.5.1
控制項	A.5.1.1 (I/P)	資訊安全政策	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。	B.1.1.1	A.5.1.1
	A.5.1.2 (I/P)	資訊安全政策之審查	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。	B.1.1.1	A.5.1.2

C級　B級　A級

A.6 資訊安全組織

本章節主要的內容可參照下表：				規範 附錄 B	原規範
A.6 資訊安全之組織					A.6 A10 A.11
控制目標	A.6.1	內部組織		条二 (B.2.1	A.6.1 A.10.1
控制項	A.6.1.1 (I/P)	資訊安全之角色及責任	應定義及配置所有資訊安全責任。	条二(三) B.2.1.1 B.2.1.2 B.2.1.3	A.6.1.1
	A.6.1.2	職務區隔	衝突之職務及責任範圍應予以區隔，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。		A.10.1.3
	A.6.1.3	與權責機關之聯繫	應維持與相關權責機關之適切聯繫。		A.6.1.4
	A.6.1.4	與特殊關注方之聯繫	應維持與各特殊關注方或其他各種專家安全論壇及專業協會之適切聯繫。		A.6.1.5
	A.6.1.5 (建議)	專案管理之資訊安全	不論專案之型式，應在專案管理中因應資訊安全。		

C級　B級　A級

A.6 資訊安全組織

控制目標	A.6.2	行動裝置及遠距工作			A.11.6
控制項	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.11.6.1 ▲
	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。		A.11.6.2 ▲

○ C級　▲ B級　◆ A級

A.7 人力資源安全

本章節主要的內容可參照下表：				規範 附錄 B	原規範
A.7 人力資源安全					A.8
控制目標	A.7.1	聘用前		B.10.1	
控制項	A.7.1.1 (I/P)	篩選	對所有可能被聘用者所進行之背景調查，應依照相關法律、法規及倫理， 並應相稱於營運要求及其將存取之資訊保密等級及組織所察覺之風險聘用。	B.10.1.1	
	A.7.1.2 (I/P)	聘用條款及條件	施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。	B.10.1.1	

A.7 人力資源安全

控制目標	A.7.2	聘用期間		B.3.1 B.10.1	A.8.2
控制項	A.7.2.1 (I/P)	管理階層責任	管理階層應要求所有員工及承包者，依施行單位所建立政策及程序施行資訊安全事宜。	B.10.1.1	
	A.7.2.2 (I/P)	資訊安全認知、教育及訓練	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。	柒四(二) 柒四(三) B.3.1.2 B.10.1.1	A.8.2.1
	A.7.2.3	懲處過程	應具備正式即已傳達之懲處過程，以對違反資訊安全之員工採取行動。		A.8.2.2

A.7 人力資源安全

控制目標	A.7.3	聘用之終止及變更		B.10.1	A.8.3
控制項	A.7.3.1 (I/P)	聘用責任之終止或變更	應對員工及承包者定義、傳達於聘用終止或變更後資訊安全責任及義務仍保持有效，並執行之。	B.10.1.1	A.8.3.1

A.8 資產管理

本章節主要的內容可參照下表：				規範 附錄 B	原規範
A.8 資產管理					A.7 A.8 A.10
控制目標	A.8.1	資產責任		B.4.1	A.7.1 A.8.3
控制項	A.8.1.1 (I/P)	資產清冊	應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。	B.4.1.1	A.7.1.1
	A.8.1.2	資產擁有權	清冊中所維持之資產應有擁有者。		A.7.1.1
	A.8.1.3	資產之可被接受的使用	對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。		A.7.1.1
	A.8.1.4	資產之歸還	所有員工及外部使用者於其聘用、契約或協議終止時，應歸還其據有之全部組織資產。		A.8.3.2

A.8 資產管理

控制目標	A.8.2	資訊分級		B.4.1 B.10.1	A.7.1 A.10.7
控制項	A.8.2.1 (I/P)	資訊之分級	資訊應依法律要求、價值、重要性及其對未經授權揭露或修改之敏感性分級。	B.4.1.2 B.10.1.1	A.7.1.2
	A.8.2.2 (I/P)	資訊之標示	應依施行單位所採用之資訊級方案，發展及實作一套適切的資訊標示程序。	B.4.1.2 B.10.1.1	A.7.1.2
	A.8.2.3 (I/P)	資產之處置	應依施行單位所採用之資訊分級方案， 發展及實作處置資產之程序。	B.10.1.1	A.10.7.3

A.8 資產管理

控制目標	A.8.3	媒體處理		B.8.1 B.10.1	A10.7
控制項	A.8.3.1 (I/P)	可移除式媒體之管理	應依施行單位所採用之資訊分級方案，實作管理可移除式媒體之程序。	B.10.1.1	A.10.7.1
	A.8.3.2 (I/P)	媒體之汰除	當不再需要媒體時，應使用正式程序加以安全汰除。	B.8.1.1 B.10.1.1	A.10.7.2
	A.8.3.3 (I/P)	實體媒體傳送	應保護含有資訊之媒體在傳送時，不受未經授權的存取、誤用或毀損。	B.10.1.1	

A.9 存取控制

本章節主要的內容可參照下表：				規範 附錄 B	原規範
A.9 存取控制					A.8,A.11 A.12
控制目標	A.9.1	存取控制之營運要求事項		B.10.1	A.11.3
控制項	A.9.1.1 (I/P)	存取控制政策	存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。	B.10.1.2	A.11.1.1
	A.9.1.2	對網路及網服務之存取	應僅提供予使用者存取其已被特定授權使用之網路及網路服務。		A.11.3.1

A.9 存取控制

控制目標	A.9.2	使用者存取管理		B.10.1	A.8.3 A.11.1
控制項	A.9.2.1 (I/P)	使用者註冊與註銷	應實作正式之使用者註冊及註銷過程， 俾能指派存取權限。	B.10.1.2	A.11.1.1
	A.9.2.2 (I/P) (建議)	使用者存取權限之配置	應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。	B.10.1.2	
	A.9.2.3 (I/P)	具特殊存取權限之管	應限制及控制具特殊存取權限之配置及使用。	B.10.1.2	A.11.1.2
	A.9.2.4 (I/P)	使用者之秘密鑑別資訊的管理	應以正式之管理過程控制秘密鑑別資訊的配置。	B.10.1.2	A.11.1.3
	A.9.2.5 (I/P)	使用者存取權限之審查	施行單位應定期審查使用者存取權限。	B.10.1.2	A.11.1.4
	A.9.2.6 (I/P)	存取權限之移除或調整	所有員工及外部使用者對資訊及資訊處理設施之存取權限， 一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。	B.10.1.2	A.8.3.3

A.9 存取控制

控制目標	A.9.3	使用者責任		B.10.1	
控制項	A.9.3.1 (I/P)	秘密鑑別資訊之使用	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。	B.10.1.2	

A.9 存取控制

控制目標	A.9.4	系統及應用存取控制		B.10.1	A.11.4 A.11.5 A.12.4
控制項	A.9.4.1 (I/P)	資訊存取限制	應根據存取控制政策， 限制對資訊及應用系統功能之存取。	B.10.1.2	A.11.5.1
	A.9.4.2 (I/P)	保全登入程序	當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。	B.10.1.2	A.11.4.1
	A.9.4.3 (I/P)	通行碼管理系統	通行碼管理系統應為互動式， 並應確保嚴謹通行碼。	B.10.1.2	A.11.4.2
	A.9.4.4	具特殊權限公用程式之使用	應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。		A.11.4.3
	A.9.4.5	對程式源碼之存取控制	應限制對程式原始碼之存取。		A.12.4.3

A.10 密碼學(加密控制)

A.10 密碼學(加密控制)					A.12
控制目標	A.10.1	密碼式控制措施(加密控制措施)		B.10.1	A.12.3
控制項	A.10.1.1 (I/P)	使用密碼式控制措施(加密控制措施)政策	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。	B.10.1.2	A.12.3.1
	A.10.1.2 (建議)	金鑰管理	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。		A.12.3.2

A.11 實體及環境安全

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.11 實體及環境安全					A.9 A11
控制目標	A11.1	安全區域		B.10.1	A.9.1
控制項	A11.1.1 (I/P)	實體安全周界	應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。	B.10.1.1	A.9.1.1
	A.11.1.2 (I/P)	實體進入控制措施	保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。	B.10.1.1	A.9.1.2
	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。		A9.1.3
	A.11.1.4	防範外部及環境威脅	應設計並施行實體保護，以防範天然災害、惡意攻擊或事故。		A.9.1.3
	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.9.1.3
	A.11.1.6 (建議)	交付及裝卸區	對諸如交付及裝卸區及其他未經授權人員可進入作業場所之進出點，應加以控制；若可能，應與資訊處理設施隔離，以避免未經授權之存取。		

A.11 實體及環境安全

控制目標	A.11.2	設備		B.8.1 B.10.1	A.9.2 A.11.2
控制項	A.11.2.1 (I/P)	設備安置及保護	應安置並保護設備， 以降低來自環境之威脅及危害造成的風險， 以及未經授權存取之機會。	B.10.1.1	A.9.2.1
	A.11.2.2	支援之公用服務事業	應保護設備免於電源失效 及因其他支援之公用服務事業失效，所導致之中斷。		A.9.2.2
	A.11.2.3	佈纜安全	應保護通訊纜線及資訊處理設備之電源，降低受竊聽或破壞的可能損失。		A.9.2.3
	A.11.2.4 (I/P)	設備維護	應正確維護設備， 以確保其持續之可用性及完整性。	B.10.1.1	A.9.2.4

A.11 實體及環境安全

	A.11.2.5 (I/P)	財產之攜出	未經事前授權，不得將設備、資訊或軟體帶出場域外。	B.10.1.1	A.9.2.7
	A.11.2.6 (建議)	場所外設備及資產的安全	安全應適用於場域外資產，並將於施行單位場所外工作之不同風險納入考量。		
	A.11.2.7 (I/P)	設備汰除或再使用之保全	含有儲存媒體之所有設備組件， 於汰除前或再使用前應加以查證，以確保任何敏感性資料及有版權之軟體已被移除或安全地覆寫。	B.8.1.1 B.10.1.1	A.9.2.5
	A.11.2.8 (建議)	無人看管之使用者設備	使用者應確保無人看管之設備具備適切保護。		
	A.11.2.9	桌面淨空及螢幕淨空政策	對紙本及可移除式儲存媒體應採用桌面淨空政策， 且對資訊處理設施應採用螢幕淨空政策。		A.11.2.1

A.12 運作安全

A.12 運作安全					A.10 A.12 A.15
控制目標	A.12.1	運作程序及責任		B.10.1	A.10.1 A.10.3
控制項	A.12.1.1	文件化運作程序	運作程序應加以文件化， 並使所有需要之使用者均可取得。		A.10.1.1
	A.12.1.2 (I/P)	變更管理	應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。	B.10.1.1	A.10.1.2
	A.12.1.3	容量管理	各項資源之使用應受監視及調適，並對未來容量要求預作規劃， 以確保所要求之系統效能。		A.10.3.1
	A.12.1.4	開發、測試及運作環境之區隔	應區隔開發、測試及運作之環境， 以降低對運作環境未經授權存取或變更的風險。		A.10.1.4 A.11.5.2

A.12 運作安全

控制目標	A.12.2	防範惡意軟體		B.10.1	A.10.4
控制項	A.12.2.1 (I/P)	防範惡意軟體之控制措施	應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。	B.10.1.1	A.10.4.1

A.12 運作安全

控制目標	A.12.3	備份		B.10.1	A.10.5
控制項	A.12.3.1 (I/P)	資訊備份	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。	B.10.1.1	A.10.5.1

A.12 運作安全

控制目標	A.12.4	存錄及監視		B.10.1 B.10.2	A.10.9
控制項	A.12.4.1 (I/P)	事件存錄	應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。	B.10.2.1	A.10.9.1 A.10.9.2 A.10.9.5
	A.12.4.2 (I/P)	日誌資訊之保護	應防範存錄設施及日誌資訊遭竄改及未經授權存取。	B.10.2.1	A.10.9.3
	A.12.4.3 (I/P)	管理者及操作者日誌	應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。	B.10.2.1	A.10.9.4
	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.10.9.6

A.12 運作安全

控制目標	A.12.5	運作中軟體之控制			A.12.4
控制項	A.12.5.1	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。		A.12.4.1

A.12 運作安全

控制目標	A.12.6	技術脆弱性管理			A.12.6
控制項	A.12.6.1	技術脆弱性管理	應及時取得關於使用中之資訊系統的技術脆弱性資訊、並應評估組織對此等脆弱性之暴露， 且應採取適當措施以因應相關風險。		A.12.6.1
	A.12.6.2 (建議)	對軟體安裝之限制	應建立並實作使用者安裝軟體之管控規則。		

A.12 運作安全

控制目標	A.12.7	資訊系統稽核考量			A.15.3
控制項	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。		A.15.3.1

A.13 通訊安全

A.13 通訊安全					A.6 A.10 A.11
控制目標	A.13.1	網路安全管理			A.10.6 A.11.3
控制項	A.13.1.1	網路控制措施	應實施網路控制措施，維護網路安全。		A.10.6.1 A.11.3.2 A.11.3.3 A.11.3.4 A.11.3.5 A.11.3.6
	A.13.1.2	網路服務之安全	應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外所提供。		A.10.6.2
	A.13.1.3	網路之區隔	應區隔各群組之資訊服務、使用者及資訊系統使用的網路。		A.11.3.4

A.13 通訊安全

控制目標	A.13.2	資訊傳送		B.6.2 B.10 B.11	A.6.1 A.10.8
控制項	A.13.2.1 (I/P)	資訊傳送政策及程序	應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。	B.6.2.1 B.6.2.2 B.10.1.1 B.11.1.1	A.10.8.1
	A.13.2.2 (I/P)	資訊傳送協議	協議應闡明組織與外部各方間營運資訊之安全傳送。	B.6.2.1 B.10.1.1 B.11.1.1	A.10.8.1
	A.13.2.3 (I/P)	電子傳訊	應適切保護電子傳訊時所涉及之資訊。	B.6.2.1 B.6.2.2 B.10.1.1 B.11.1.1	A.10.8.2
	A.13.2.4 (I/P)	機密性或保密協議	應識別、定期審查及文件化，以反映施行單位對資訊保護之需要的機密性或保密協議之要求事項。		A.6.1.3

A.14 系統獲取、開發及維護

本章節主要的內容可參照下表：				規範 附錄 B	原規範
A.14 系統獲取、開發及維護					A.10 A.12
控制目標	A.14.1	資訊系統之安全要求事項			A.10.8 A.12.1
控制項	A.14.1.1 (I/P)	資訊安全要求事項分析及規格	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。	B.10.1.1	A.12.1.1
	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.10.8.4
	A.14.1.3 (建議)	保護應用服務交易	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

控制目標	A.14.2	於開發及支援過程中之安全			A.12.5
控制項	A.14.2.1 (建議)	保全開發政策	應建立軟體及系統開發之規則，並應用至施行單位內之開發。		
	A.14.2.2	系統變更控制程序	應藉由使用正式之變更控制程序，以控制開發生命周期內之系統變更。		A.12.5.1
	A.14.2.3	運作平台變更後，應用之技術審查	當運作平台變更時，應審查及測試營運之關鍵應用，以確保對組織運作或安全無不利衝擊。		A.12.5.2
	A.14.2.4	軟體套件變更之限制	應不鼓勵修改軟體套件， 且僅限於必要變更，並應嚴格控制所有變更。		A.12.5.3
	A.14.2.5	保全系統工程原則	保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。		A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.4
	A.14.2.6 (建議)	保全開發環境	對涵蓋整個系統開發生命周期之系統開發及整合工作，施行單位應建立並適切地保護安全開發環境。		
	A.14.2.7	委外開發	組織應監督及監視委外系統開發活動。		A.12.5.5
	A.14.2.8 (I/P) (建議)	系統安全測試	於開發中，應實施安全功能之測試。	B.10.1.1	
	A.14.2.9 (I/P)	系統驗收測試	應建立新資訊系統、系統升級及新版本之驗收測試計畫及準則。	B.10.1.1	

A.14 系統獲取、開發及維護

控制目標	A.14.3	測試資料			A.12.4
控制項	A.14.3.1 (I/P)	測試資料之保護	應小心選擇、保護及控制測試資料。	B.10.1.1	A.12.4

A.15 供應者關係

本章節主要的內容可參照下表：				規範 附錄 B	原規範
A.15 供應者關係					A.6 A.10
控制目標	A.15.1	供應者關係中之資訊安全		B.12.1	A.6.2
控制項	A.15.1.1 (I/P)	供應者關係之資訊安全政策	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。	B.12.1.1	
	A.15.1.2 (I/P)	於供應者協議中闡明安全性	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。	B.12.1.2	A.6.2.1
	A.15.1.3 (I/P) (建議)	資訊及通訊技術供應鏈	與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。	B.12.1.2	

A.15 供應者關係

控制目標	A.15.2	供應者服務交付管理		B.12.1	A.10.2
控制項	A.15.2.1 (I/P)	供應者服務之監視及審查	組織應定期監視、審查及稽核供應者服務交付。	B.12.1.1	A.10.2.2
	A.15.2.2 (I/P)	管理供應者服務之變更	應管理供應者所提供服務之變更，包括維持及改善既有的資訊安全政策、程序及控制措施，並考量所涉及之營運資訊、系統及過程的關鍵性，以及風險之重新評鑑。	B.12.1.1	A.10.2.3

A.16 資訊安全事故管理

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.16 資訊安全事故管理					A.13
控制目標	A.16.1	資訊安全事故及改善之管理		B.10.2	A.13.1 A.13.2
控制項	A.16.1.1 (I/P)	責任及程序	應建立管理責任及程序， 以確保對資訊安全事故做迅速、有效及有序之回應。	B.10.2.1	A.13.2.1
	A.16.1.2 (I/P)	通報資訊安全事件	應循適切之管理管道，儘速通報資訊安全事件。	B.10.2.1	A.13.1.1
	A.16.1.3 (I/P)	通報資訊安全弱點	應要求使用資訊系統及服務之員工及承包者，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。	B.10.2.1	A.13.1.1
	A.16.1.4 (I/P)	資訊安全事件評估及決策	應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。	B.10.2.1	
	A.16.1.5 (I/P)	對資訊安全事故之回應	應依文件化程序，回應資訊安全事故。	B.10.2.1	
	A.16.1.6 (I/P)	由資訊安全事故中學習	應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性及衝擊。	B.10.2.1	A.13.2.2
	A.16.1.7 (I/P)	證據之收集	組織應定義及應用程序，以識別、蒐集、取得及保存可用作證據之資訊。	B.10.2.1	A.13.2.3

A.17 營運持續管理之資訊安全層面

本章節主要的內容可參照下表：				規範 附錄 B	原規範
A.17 營運持續管理之資訊安全層面					A.14
控制目標	A.17.1	資訊安全持續			A.14.1
控制項	A.17.1.1	規劃資訊安全持續	施行單位應決定對其資訊安全之要求事項，以及在不利情況下（例：危機或災難期間），對資訊安全之持續性要求事項。		A.14.1.1
	A.17.1.2	實作資訊安全持續	施行單位應建立、文件化、實作及維持過程、程序及控制措施，以確保在不利情況期間所要求之資訊安全持續等級。		A.14.1.1
	A.17.1.3	查證、審查及評估資訊安全持續	組織應定期查證所建立及實作之資訊安全持續控制措施，以確保其於不良情況期間係生效及有效。		A.14.1.2

A.17 營運持續管理之資訊安全層面

控制目標	A.17.2	多重備援			
控制項	A.17.2.1	資訊設備之可用性	應對資訊處理設施實作充分之多重備援，以符合可用性要求。		

A.18 遵循性

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.18 遵循性					A.6 A.15
控制目標	A.18.1	對法律及契約要求事項之遵循		第一(一)	A.15.1
控制項	A.18.1.1 (I/P)	適用之法規及契約的要求事項之識別	對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項 以及組織為符合此等要求之作法。	第一(一) B.11.1.2	A.15.1.1
	A.18.1.2	智慧財產權	應實作適切程序， 以確保遵循智慧財產權及專屬軟體產品使用之相關法律、法令及契約的要求事項。	第一(一)	A.15.1.2
	A.18.1.3 (I/P)	紀錄之保護	應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未授權存取及未經授權發布。	B.10.1.1	A.15.1.2
	A.18.1.4 (I/P)	個人可識別資訊之隱私及保護	應依適用之相關法令、法規中之要求，以確保符合個人可識別資訊之隱私及保護。	B.10.1.1	A.15.1.2
	A.18.1.5 (建議)	密碼式控制措施(加密控制措施)的監管	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。	第一(一)	

A.18 遵循性

控制目標	A.18.2	資訊安全審查		柒六(二) 柒六(三) B.10.1	A.6.1 A.15.2
控制項	A.18.2.1 (I/P)	資訊安全之獨立審查	應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全之作法及其實作（亦即資訊安全之各項控制目標、控制措施、政策、過程及程序）。	柒六(三) B.10.1.3	A.6.1.6
	A.18.2.2 (I/P)	安全政策及標準之遵循性	管理人員應以適切之資訊安全政策、標準及其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。	柒六(二) B.10.1.3	A.15.2.1
	A.18.2.3 (I/P)	技術遵循性審查	應定期審查資訊系統對組織之資訊安全政策及標準的遵循性。	柒六(二) B.10.1.3	A.15.2.2

謝謝
聆聽

Question
& Answer ...

NII 產業發展協進會
☏ (02) 2508-2353
✉ 台北市松江路 317 號 7 樓