教育機構資安驗證中心

「教育體系資通安全暨個人資料管理規範」改版說明

主講人

國立中興大學計算機及資訊網路中心主任 陳育毅

台灣檢驗科技股份有限公司產品部經理 曾蕙瑜

大　　綱

一、依循國際標準並參考相關法令
二、新版規範特色
三、新舊版本差異
四、教版規範導入與選定控制措施
五、轉版執行進程
六、教育體系資通安全暨個人資料管理規範說明

依循國際標準並參考相關法令

國際標準

- ISO27001:2013 Information security management systems-Requirements.
- ISO27002:2013 Code of practice for information security controls.
- BS10012:2009 Data Protection Specification for a Personal Information Management.
- ISO29100:2011 Information technology-Security techniques-Privacy framework.
- ISO29101:2013 Information technology-Security techniques-Privacy architecture framework.
- ISO29191:2012 Information technology-Security techniques-Requirements for partially anonymous, partially unlinkable authentication.

依循國際標準並參考相關法令

資安法令規範

- 政府機關(構)資通安全責任等級分級作業規定
- 教育體系機關(構)及學校單位資通安全責任等級分級表
- 資訊系統分類分級與鑑別機制參考手冊
- 政府機關構資安事件數位證據保全標準作業程序

個人資料管理

- 個人資料保護法及個人資料保護法施行細則
- 教育機構個人資料保護工作事項
- 教育體系個人資料安全保護基本措施
- 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

新版規範特色

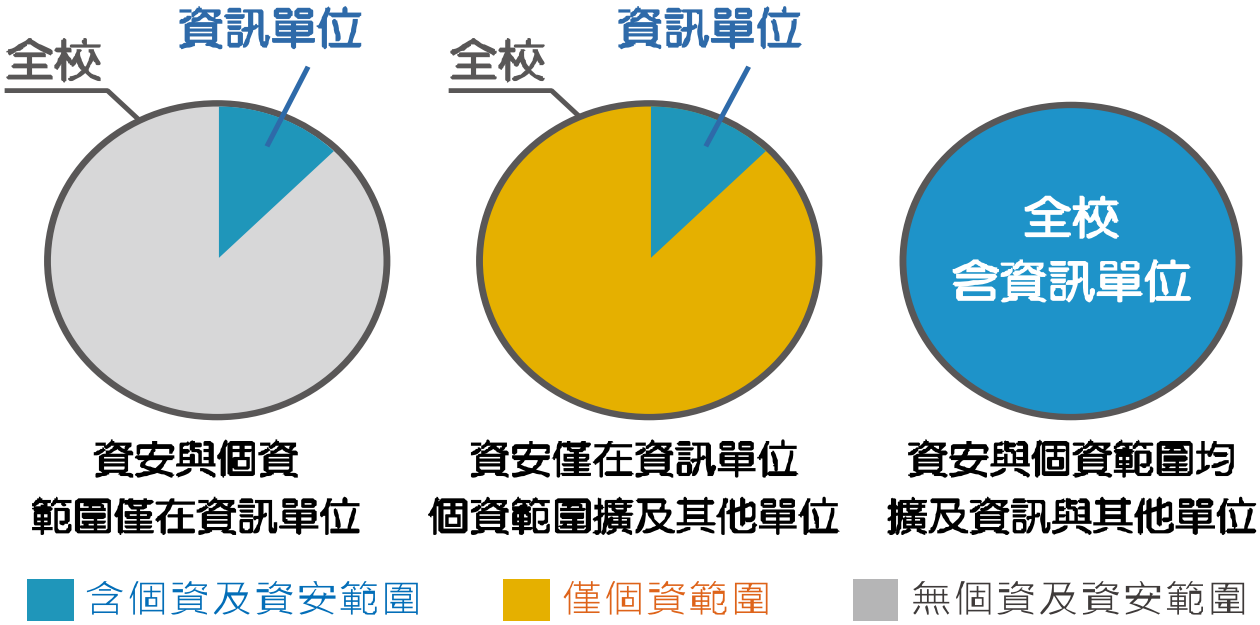
- 資安規範 ＋ 個資規範
- 參考國際標準並篩選適合教育機構之控制措施
- 依據資通安全責任等級融入適用之實作指引
- 建立單一驗證標準

新舊版本差異

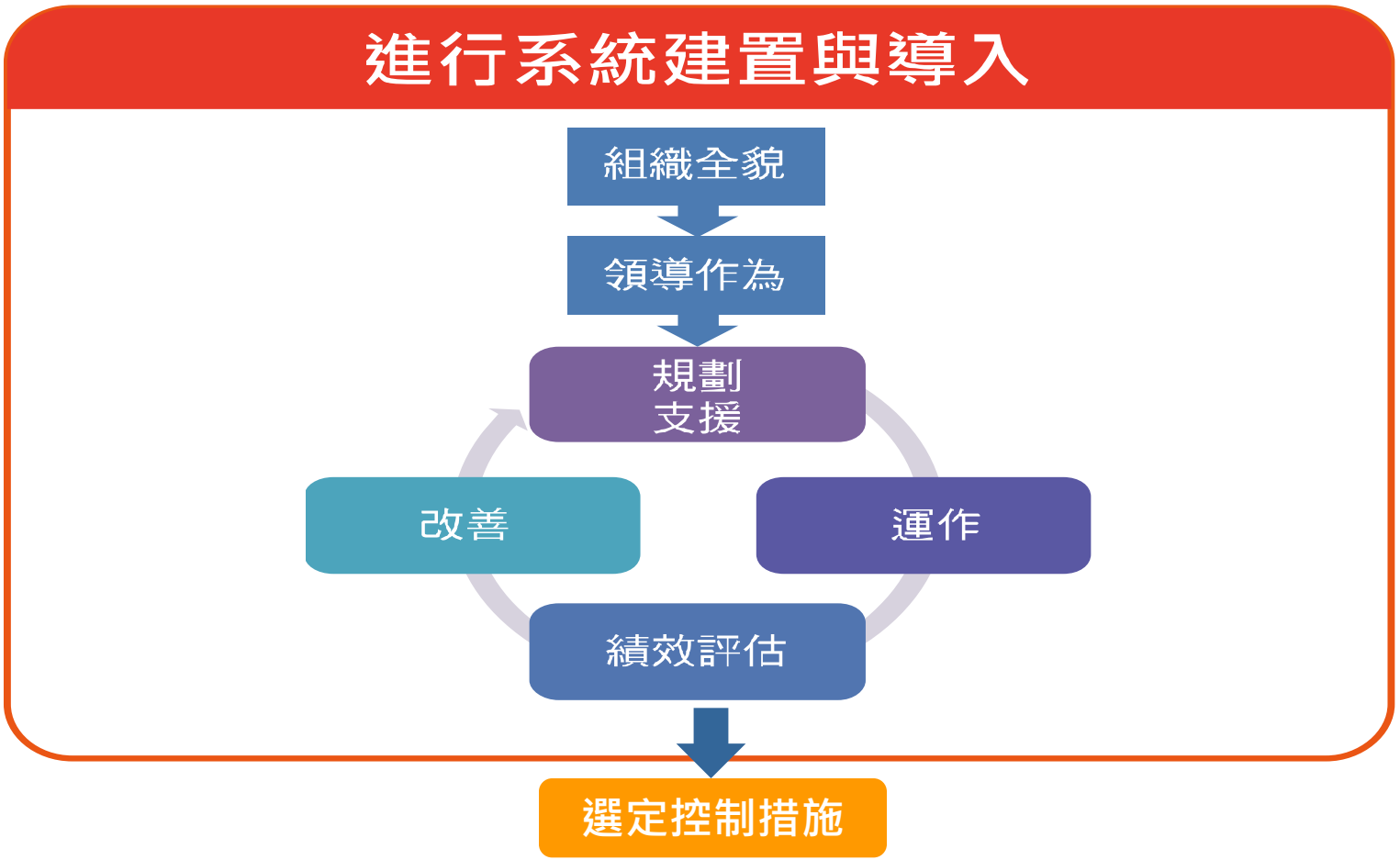
教育體系資通安全暨個人資料管理規範	舊　　版	新　　版
建置步驟與需求	捌、三~玖、十	柒、一~七
適用性聲明書(SoA)	✓	✓
附錄控制項(Annex A)	✓	✓
控制領域條款	A.5~A.15	A.5~A.18
控制領域數	11	14
控制目標數	36	35
控制項數目	100	114
學群/等級	第一/二學群	A/B/C

教版規範導入

選定導入範圍



教版規範導入



教版規範導入

選定控制措施

轉版執行進程

規範草案公告

- 成果說明會
- 教育體系資訊主管會議
- 規範巡迴說明講座
- 網站公告（線上問卷）

新版導入

- 資安規範稽核員轉版教育訓練
- 教育體系資安與個資保護管理規範轉版導入說明
- 教育體系資安與個資保護管理規範整合導入說明
- 個資規範稽核員教育訓練

教育機構轉版施行

- 承辦人員轉版訓練
- 確認新版適用性聲明
- 制度文件與控制措施調整
- 內部稽核

轉版驗證稽核

- 教育機構資安規範轉版申請
- 資安規範稽核員轉版觀察
- 資安規範稽核員轉版稽核

教育體系資通安全暨個人資料管理規範（草案第三版）先期導入自評暨問卷調查

http://tcnc.tw/8VKYg

教育體系資通安全暨個人資料管理規範說明

管理規範說明

一、簡介
二、適用範圍
三、目標期程
四、引用標準
五、關於適用性聲明
六、建置步驟及需求

簡介

教育體系資通安全暨個人資料管理規範
（資安/個資共用 均須遵循）

附錄A
資訊安全管理規範
（資安選用）

附錄B
個人資料管理規範
（個資選用）

附錄 C
個人資料保護規範對照表

附錄D
規範詞彙與定義

規範實施自評/查檢表

參考附錄
隱私強化技術
（參考文件）

規範實施自評/查檢表

- 採用單一整合管理制度與組織架構
- 可依據管理制度規劃選用管理規範
  - 僅選用資通安全管理規範
  - 僅選用個人資料管理規範
  - 選用整合性管理規範

建議適用範圍

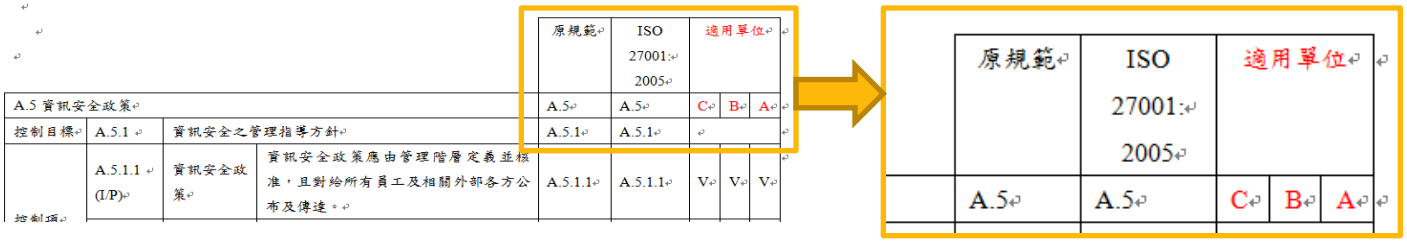
各機構依據「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」所屬等級選定適用範圍，應至少包含下列建議範圍

	ISMS	PIMS
A級	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部門，或試務管理部門。	全單位所有個人資料處理流程。
B級	應至少包含資訊管理部門、學術網路系統、核心業務資訊系統。	應至少包含涉及核心業務之個人資料處理流程之行政單位，以及資訊管理單位。
C級	應至少包含資訊管理單位及校務行政資訊系統。	應至少包含資訊管理單位，核心業務之個人資訊管理業務。

適用性聲明

- 適用ISMS單位

  可依據適用單位等級選擇控制措施，參考附錄A之控制措施，產生「ISMS適用性聲明」。各等級單位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，且排除後不影響該單位提供資通安全能力與責任之控制措施。



			原規範	ISO 27001:2005	適用單位		
A.5 資訊安全政策			A.5	A.5	C	B	A
控制目標	A.5.1	資訊安全之管理指導方針	A.5.1	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。	A.5.1.1	A.5.1.1	V	V	V

原規範	ISO 27001:2005	適用單位		
A.5	A.5	C	B	A

適用性聲明

- 適用PIMS單位

  應選用附錄B所有控制項。

- 整合「資通安全管理暨個人資料管理系統」

  應同時遵循ISMS & PIMS 要求，並建立「資通安全管理暨個人資料管理系統適用性聲明」。

教育機構驗證要求

- 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。

建置步驟與架構

單一管理系統架構
所有制度施行單位均依循
本建置步驟要求

配合ISO管理制度標準
發展趨勢強調組織發
展架構與流程

附錄A. B的控制措施

控制項編號下(I/P)註記代表ISMS與PIMS可共用項目。

附錄A 資訊安全管理規範 (資安選用)	附錄B 個人資料管理規範 (個資選用)

• 控制領域A.5~A.18
  • 控制目標
  • 控制項
  • 實作指引
	• 控制領域 B.1~B.12
	  • 控制目標
	  • 控制項
	  • 實作指引

附錄A 資訊安全管理規範（資安選用）

附錄A資訊安全管理規範新舊版本差異

新版資安規範	原有資安規範
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 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.7資訊資產分類與管制
A.9 存取控制	A.11存取控制安全
A.10 密碼學(加密控制)	
A.11 實體及環境安全	A.9實體與環境安全
A.12 運作安全	A.10通訊與作業安全管理
A.13 通訊安全	A.10通訊與作業安全管理
A.14 系統獲取、開發及維護	A.12系統開發與維護之安全
A.15 供應者關係	
A.16資訊安全事故管理	A.13資訊安全事件之反應及處理
A.17業務永續運作管理	A.14業務永續運作管理
A.18遵循性	A.15相關法規與施行單位政策之符合性
14控制領域	11控制領域

新增適用控制措施

1. 原規範為刪除之控制措施

控制項			原規範	ISO 27001:2005	適用單位		
					C	B	A
A.7.1.1	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。		A.7.1.2		V	V
A.7.1.2	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。		A.7.1.3	V	V	V
A.8.3.3	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。		A.10.8.3		V	V
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。		A.11.1.1		V	V
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。		A.11.3.1	V	V	V

新增適用控制措施

2. ISO 27001:2013新增或修訂後納入之控制措施

控制項			原規範	ISO 27001:2005	適用單位		
					C	B	A
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.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.4		V	V
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。				V	V
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。			V	V	V
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。			V	V	V
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。				V	V

新增適用控制措施

3. B級單位「高」等級資訊系統應納入之控制措施

控制項			原規範	ISO 27001:2005	適用單位		
					C	B	A
A.14.1.3	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.10.9.2			V
A.14.2.1	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。					V
A.14.2.6	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。					V
A.14.2.8	系統安全測試	於開發中，應實施安全功能之測試。					V
A.15.1.3(I/P)	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。					V

刪除之適用控制措施(I)

原規範	控制項		ISO27001:2005	ISO27001:2013
A.6.1.2	資訊設施使用之授權	資訊處理設備的移轉(包含新設備)，應由權責主管人員進行授權、移交的程序，確保該設備後續的順利運作以及責任所屬。	A.6.1.4	刪除
A.10.7.3	資料檔案之保護	重要資料檔案應進行控管，並安全的保存。	A.10.7.3	刪除
A.10.7.4	系統文件之安全	重要系統文件應受到保護，避免未授權之存取。	A.10.7.4	刪除
A.11.3.2	遠端使用者身份鑑別	遠端連線使用者之存取需進行身分鑑別。 —較適用於第一群	A.11.4.2	併入A13.1.1
A.11.3.3	診斷埠(Diagnostic Ports)存取控制	診斷埠的存取行為必須嚴密控管。 —較適用於第一群	A.11.4.4	併入A13.1.1
A.11.3.4	網路分隔控制	網路應視需求控制措施，將資訊服務、使用者及各資訊系統區隔。 —較適用於第一群	A.11.4.5	併入A13.1.1
A.11.3.5	網路連線控制	使用者連線能力應視需求予以限制。 —較適用於第一群	A.11.4.6	併入A13.1.1
A.11.3.6	網路路由控制	共享網路應有路由控制措施，確保電腦連線及資訊流依循應用系統之存取控管政策。 —較適用於第一群	A.11.4.7	併入A13.1.1
A.11.4.4	連線作業時間之控制	必要時限制使用者在高風險應用系統的連線作業時間。 —較適用於第一群	A.11.5.6	併入A13.1.1

刪除之適用控制措施(II)

原規範	控制項		ISO27001:2005	ISO27001:2013
A.11.5.2	機密及敏感性系統之獨立作業	必要時對機密性及敏感性系統，考量建置獨立的或是專屬的電腦作業環境。 —較適用於第一群	A.11.6.2	併入A.12.1.4
A.12.2.1	資料輸入之驗證	輸入應用系統之資料須確認其正確性與適當性。	A.12.2.1	併入A.14.2.5
A.12.2.2	系統內部作業處理之驗證	系統需建立確認檢查機制，以偵知所處理資料的塗改。	A.12.2.2	併入A.14.2.5
A.12.2.3	訊息真確性之鑑別	必要時應採用訊息鑑別機制，保護訊息內容的完整性。 —較適用於第一群	A.12.2.3	併入A.14.2.5
A.12.2.4	資料輸出控管	應用系統的資料輸出需經過確認，確保處理程序的正確性與適當性。	A.12.2.4	併入A.14.2.5
A.12.5.4	資訊洩漏控制	預防施行單位資訊遭洩漏的危機，制定適當的控管措施。 —較適用於第一群	A.12.5.4	併入A.14.2.5
A.15.3.2	系統稽核工具之保護	系統稽核之相關工具需建立適當的保護措施，並視需求設立備援及緊急應變方案。	A.15.3.2	刪除

附錄A 資訊安全管理規範特色

- 延用原有規範架構，並列出原編號 方便使用者參照
- 依ISO 27001:2013控制領域、目標與控制項列舉，便於比較，並參照ISO 27002:2013資訊安全措施之作業規範建議，提供實作參考
- 結合政府機關相關資訊安全措施要求
  - 教育體系機關構及學校資通安全責任等級分級作業規定
  - 資訊系統分級與資安防護基準作業規定
  - 政府機關構資安事件數位證據保全標準作業程序
- 可依據資訊系統分級鑑別結果選用控制措施，提供施行單位依風險狀況彈性選擇

附錄A 資訊安全管理規範規劃

- 援引原有學群分類方式
  - 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。
- 教育體系機關構及學校資通安全責任等級分級
  - A級單位：適用所有控制措施(計114項)
  - B級單位：適用原第一學群之控制措施(計101項)
  - C級單位：適用原第二學群之控制措施(計51項)
  - 國中小學建議依循國中小學資通安全管理實施原則所規範之控制措施(計29項)

附錄A 管理規範格式說明(一)

控制領域

A.18
遵循性

控制領域說明

所有的 ISMS 控制措施與管理條款，除了須符合施行單位的政策外，與相關法規的符合性亦須相符，避免缺乏法源上的依據，而在於系統方面的稽核上，也需採用適當的工具進行檢測，確保運作維持不中斷。

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

可整合規範建置步驟與附錄B控制項編號

控制目標

可共用註記（I/P）

原規範控制項編號

附錄A 管理規範格式說明(二)

實作指引	
控制目標	(一) 資訊安全之管理指導方針 (A.5.1)
控制項	1. 資訊安全政策 (A.5.1.1)
控制項說明	資訊安全政策應參考資訊安全相關法令及施行單位業務上的需求，並經由管理階層核准，以適當方式向所有員工公佈與宣導，在必要時告知相關單位及合作廠商，以利共同遵守。
參考項說明	施行單位制定資訊安全政策，應說明管理階層的承諾及該單位管理資訊安全的方法，宜涵括下列事項： (1) 資訊安全之定義、整體目標、範圍，及進行資訊共享時，其安全機制的重要性。 (2) 資訊安全政策宜包含法令及契約對施行單位資訊安全的要求與規定。 (3) 資訊安全政策宜包含資訊安全教育及訓練的要求。

附錄A 管理規範格式說明(三)

如有資通安全責任分級作業或相關資安規定要求者，則將會於控制項中說明應遵循要求執行。

（一）內部組織（A.6.1）

1. 資訊安全之角色及責任（A.6.1.1）

應定義及配置所有資訊安全責任。

施行單位應由副首長擔任或指定管理制度之管理人或召集人，並應依據「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」或相關資安規定中各級單位資安專責人力要求進行指派。

由 ISMS 管理人與管理小組舉辦之定期（宜每半年）資訊安全會報，召集相關單位代表進行工作與責任的分派，確保資訊安全相關計畫的進行，並展現管理階層的支持。

定期（宜每半年）召開之資訊安全會報權責宜包含：

(1) 訂定資訊安全角色與權責分工，賦予相關人員應有之安全權責，包含資訊安全相關政策、計畫、措施、技術規範、安全技術研究、建置、評估，乃至使用管理、保護、資訊機密維護、稽核等，並以書面或其他方式記錄留存。

(2) 確保安全活動符合資訊安全政策。

(3) 資訊安全教育訓練及認知之提昇。

(4) 評估資訊安全事項審查及監視的結果，並針對資訊安全事故提出適當的行動方案。

教育機構資安驗證中心

各級教育機構適用控制項對照

附件1各級教育機構適用控制項對照表

	原規範	ISO 27001:2005	適用單位		
	A.5	A.5	C	B	A

適用單位

				原規範	ISO 27001:2005	適用單位		
A.5 資訊安全政策				A.5	A.5	C	B	A
控制目標	A.5.1	資訊安全之管理指導方針		A.5.1	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。	A.5.1.1	A.5.1.1	V	V	V
控制項	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。	A.5.1.2	A.5.1.2	V	V	V
A.6 資訊安全之組織				A.6/A10.1 A.11	A.6			
控制目標	A.6.1	內部組織		A.6.1 A.10.1	A.6.1 A.8.1 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。	A.6.1.1	A.6.1.3 A.8.1.1	V	V	V
控制項	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.10.1.3		V	V
控制項	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.6.1.6	V	V	V
控制項	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.6.1.7	V	V	V
控制項	A.6.1.5	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。					V

依據教育部與所屬機關(構)及學校資通安全責任等級分級適用

附錄B 個人資料管理規範（個資選用）

附錄B個人資料管理規範特色

- 延用原有教育體系資安管理規範架構， 方便參照
- 依據BS10012:2009條款列舉，並增列BS10012:2009與ISO 29100:2011條款編號，俾便施行單位參考外界常見個資管理標準與要求
- 結合政府機關相關資訊安全措施要求
  - 個人資料保護法及個人資料保護法施行細則
  - 教育體系個人資料安全保護基本措施
  - 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
- 參照個人資料管理導入與實作經驗建議作業方式，提供實作參考

附錄B個人資料管理規範控制領域

B.1 個人資料 管理政策	B.2 個人資料 管理組織	B.3 人員認知與訓練	B.4 個人資料之 識別與風險管理
B.5 公正與合法 的處理	B.6 個人資訊 特定目的處理	B.7 適當相關 與正確性	B.8 保存與處置
B.9 當事人權利	B.10 資料安全議題	B.11 國際傳輸	B.12 委外管理

教育機構資安驗證中心

附錄B 管理規範格式說明(一)

控制領域

B.2

個人資料管理組織

控制領域說明

為於落實個人資料管理政策，施行單位應建立個人資料管理組織及管理窗口網絡，以促進各項管理程序與規範的正確執行。指定適當權責之高層主管人員肩負個人資料管理責任，除展示學校或單位落實個人資料管理的決心外，更能自管理階層的高度及管理邏輯，確保個人資料管理權責委派予適當同仁，並提供必要資源強化現行作業成效，以建立完善且安全之作業環境，降低個人資料管理風險。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.2 個人資料管理組織					
控制項	B.2.1	內部組織		条二 A.6.1	§18 細§12
	B.2.1.1 (I/P)	管理階層角色及責任	應由管理階層負責個人資料管理，確保個人資料保護法令及良好實務的遵循	条二(一) A.6.1.1	細§12
	B.2.1.2 (I/P)	日常作業管理責任	指派合格或具經驗的人員，確保日常作業符合個人資料管理相關政策的要求	条二(三) A.6.1.1	§18 細§12
	B.2.1.3 (I/P)	個人資料管理專人	建立各單位的個人資料管理窗口，協助個人資料相關日常作業的執行	条二(三) A.6.1.1	§18 細§12

控制目標

可整合規範建置步驟與附錄A控制項編號

個資法條款編號

可共用註記 (I/P)

附錄B 管理規範格式說明(二)

實作指引	
控制目	(一)個人資料管理方針(B.1.1)
控制項	1. 個人資料管理政策(B.1.1.1)
控制項說明	施行單位應訂定文件化的個人資料管理政策，經最高管理階層核定，並傳達至所有員工，以展現對遵循個人資料保護法律與良好實務的支持與承諾。個人資料管理政策應每年、依管理階層指示或重大變更發生時，重新審查。
參考項說明	個人資料管理政策之內容，宜包含以下資訊與承諾： (1) 僅基於施行單位合法目的下，進行必要的個人資料處理； (2) 僅針對特定目的蒐集最小化的個人資料，且不處理過多的個人資料； (3) 明確提供當事人其個人資料使用方式與對象的資訊； (4) 僅處理相關且適當的個人資料； (5) 公平與合法的處理個人資料； (6) 維護個人資料分類清冊； (7) 保持個人資料的正確性，並依需要保持最新； (8) 僅依法律或施行單位合法目的的要求下，保存個人資料； (9) 尊重當事人行使其當事人權利； (10) 維護所有個人資料的安全；

教育機構資安驗證中心

個人資料控制措施與各項標準對照

附件 1 附錄 B 個人資料控制措施與各項標準對照表

個人資料控制措施				規範附錄 A	個資法	BS10012:2009	ISO29100:2011
B.1 個人資料管理政策							
控制目標	B.1.1	個人資料管理方針		条二(二) A5.1		3.3 3.4	4.6
控制項	B.1.1.1 (I/P)	個人資料管理政策	核准並定期審查個人資料管理政策，展現管理階層對遵循個人資料保護法律及良好實務的承諾	条二(二) A5.1.1 A.5.1.2		3.3 3.4	4.6
B.2 個人資料管理組織							
控制目標	B.2.1	內部組織		条二 A.6.1	§18 細§12		
控制項	B.2.1.1 (I/P)	管理階層角色及責任	應由管理階層負責個人資料管理，確保個人資料保護法令及良好實務的遵循	条二(一) A.6.1.1	細§12	3.5 4.1.1	
	B.2.1.2 (I/P)	日常作業管理責任	指派合格或具經驗的人員，確保日常作業符合個人資料管理相關政策的要求	条二(三) A.6.1.1	§18 細§12	4.1.2 4.5	

附錄C個人資料保護規範對照表

教育機構個人資料保護工作事項檢核對照表

個資法施行細則11項安全維護事項要求對照表

附錄 C

個人資料保護規範對照表

一、 教育機構個人資料保護工作事項檢核對照表

查核項目	教育體系資通安全暨個人資料管理規範	附錄A 資訊安全管理規範	附錄B 個人資料管理規範
一、規劃			
1. 配置個人資料管理之人員及相當資源			
1.1 是否建立個人資料保護管理政策？	柒、二、(二)建立政策與目標		B.1.1.1 個人資料管理政策
1.2 是否成立個人資料保護管理小組，並由單位副首長擔任機關召集人？	柒、二、(一)領導及承諾		B.2.1.1管理階層角色及責任
1.3 是否指定專人依法令規定辦理個人資料安全維護及保管事項？	柒、二、(三)組織角色、責任與授權		B.2.1.2日常作業管理責任 B.2.1.3個人資料管理專人
1.4 是否決定並提供單位規劃與施行個人資料保護工作所需的資源，包含人力、物資或外部諮詢顧問等？	柒、四、(一)資源		

二、 個資法施行細則 11 項安全維護事項要求對照表

個資法 安全維護事項	ISO 27001:2013	BS10012:2009	ISO 29100:2011
配置管理之人員及相當資源	5.3組織角色、責任與授權 7.1資源	3.5職責與歸責性 3.6 資源提供 4.1重要職責指派	5.10歸責性
界定個人資料之範圍	4.3決定資訊安全管理系統範圍	3.2 PIMS的範圍與目標	4.2行為者及角色 4.3互動 4.4辨識PII
個人資料之風險評估及管理機制	6.1風險與機會處理措施	4.4風險評鑑	4.5隱私保全要求事項
事故之預防、通報及應變機制	6.1風險與機會處理措施 附錄A 全 A.16資訊安全事故管理 A.17 營運持續管理 資訊安全層面	4.7公平與合法的處理 4.13安全議題	4.6 隱私權政策 4.7隱私控制措施

附錄D 規範詞彙與定義

- 配合教育體系資通安全暨個人資料管理規範，以及附錄提供名詞說明

附錄 D

規範詞彙與定義

存取控制 ACCESS CONTROL
用以確保資產存取是基於營運與安全要求經授權且限制的方法。

ISO/IEC 27000:2014

可歸責性 ACCOUNTABILITY
個體對其行動與決策的職責

ISO/IEC 27000:2014

資產 ASSET
對於組織有價值的事物
備註：資產有很多類型，包含
a) 資訊；
b) 軟體，例如電腦程式；
c) 實體，例如電腦；
d) 服務；
e)人員，與他們的資格、技術與經驗；及
f)無形資產，如聲譽與形象。

ISO/IEC 27000:2014

參考附錄 隱私強化技術介紹

- 參考標準
  - 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
- 配合個人資料管理系統與隱私資訊管理需求提供技術參考

識別資通訊系統個資處理框架

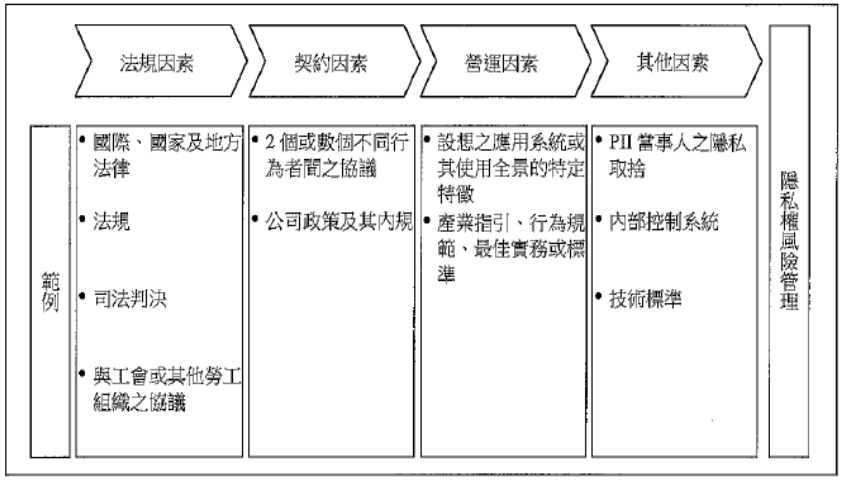
資料來源: ISO/IEC 29101:2013 Information technology — Security techniques — A privacy reference architecture

識別資通訊系統隱私保全要求事項決定因素

- 法規/契約
- 營運/其他

識別資通訊系統個人資料處理流程中的

- 行為者及角色
- 互動
- 辨識個人可識別資訊(PII)
- 隱私保全要求事項
- 個人資料(隱私權)政策
- 個人資料(隱私)控制措施

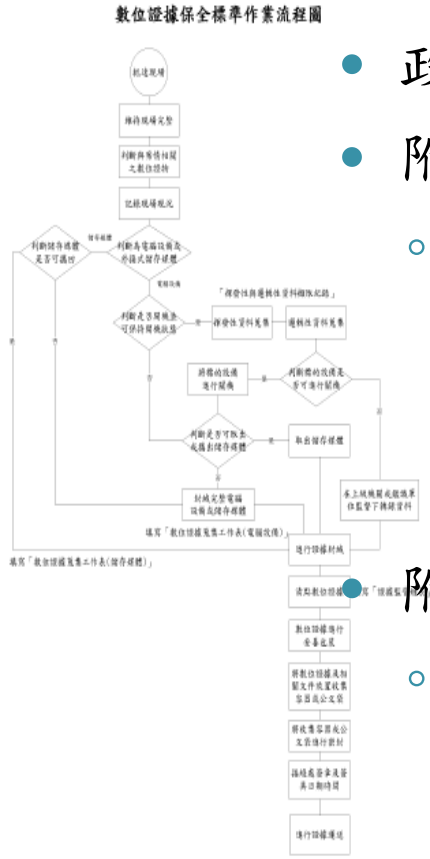


資料來源：ISO 29100:2011資訊技術－安全技術－隱私權框架
Information technology − Security techniques − Privacy framework

設計個人資訊隱私技術

- 個資最小化技術
  - 假(化)名化(Pseudonymization)
  - 匿名化(Anonymization)
  - 不可觀察性資料管理(Unobservable data management)
  - 查詢限制技術
- 個資當事人授權措施
  - 當事人之同意授權
- 資料存取控制、儲存與處理之安全措施
  - 生物特徵加密(Biometric encryption)
  - 秘密分享(Secret sharing)
  - 安全性多方計算(Secure multi-party computation, MPC)

資安事件數位證據保全



- 政府機關(構)資安事件數位證據保全標準作業程序
- 附錄A 資訊安全管理規範
  - 證據之收集（A.16.1.7）
    - 如發生資訊安全事故，應依據「政府機關（構）資安事件數位證據保全標準作程序」進行數位證據之蒐集與保存，

附錄B 個人資料管理規範

- 安全事故管理程序與紀錄(B.10.2.1)
  - 發生安全事故時，應依據「政府機關（構）資安事件數位證據保全標準作業程序」進行數位證據之蒐集與保存。

Q & A