ISO27001：2013轉版

課程大綱

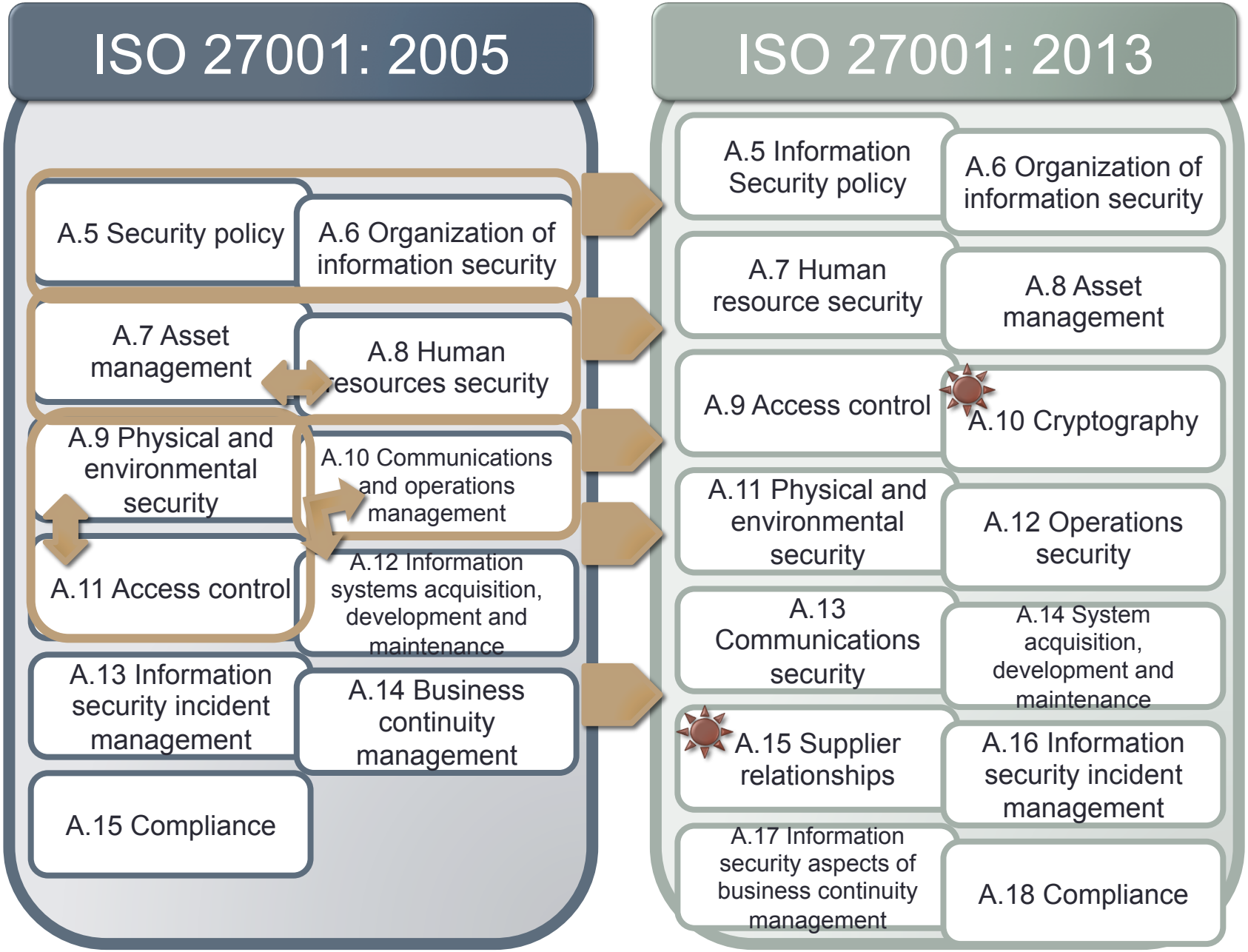
- ISO27001架構
- 本文架構
- 附錄架構
- 4.組織環境
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.
- 附錄A
- 條文A.5~A.18

DAY 2

ISO 27001:2013 Annex A

14領域;35控制目標;114控制項目

- A.5 Information Security Policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

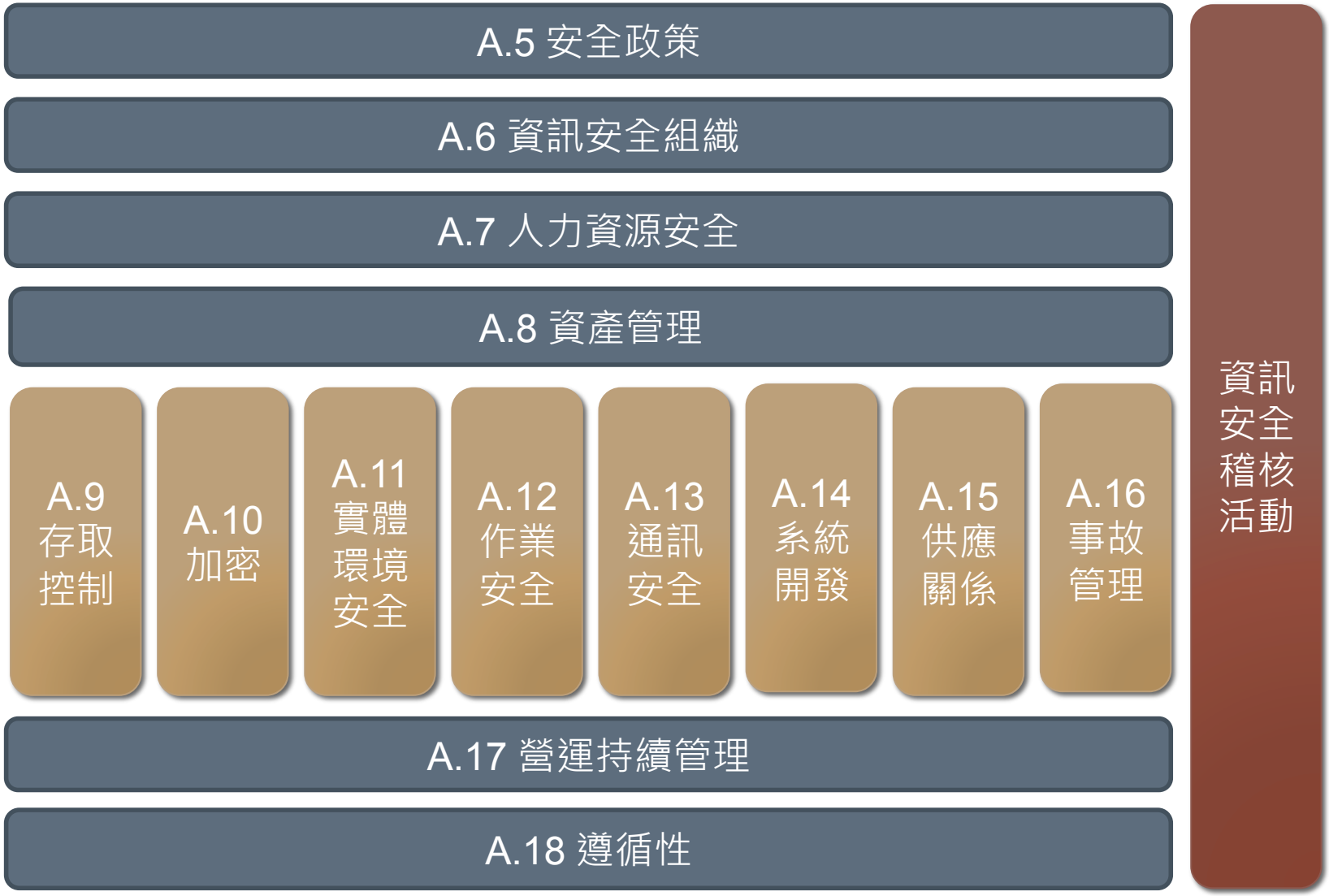

ISO 27001: 2005
A.5 Security policy
A.6 Organization of information security
A.7 Asset management
A.8 Human resources security
A.9 Physical and environmental security
A.10 Communications and operations management
A.11 Access control
A.12 Information systems acquisition, development and maintenance
A.13 Information security incident management
A.14 Business continuity management
A.15 Compliance
ISO 27001: 2013
A.5 Information Security policy
A.6 Organization of information security
A.7 Human resource security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 System acquisition, development and maintenance
A.15 Supplier relationships
A.16 Information security incident management
A.17 Information security aspects of business continuity management
A.18 Compliance

2013附錄A	Objective	Control	2005附錄A
A.5 Information security policy	1	2	A.5 Security Policy
A.6 Organization of information security	2	7	A.6 Organization
A.7 Human resource security	3	6	A.8 Human resource
A.8 Asset management	3	10	A.7 Asset management
A.9 Access control	4	14	A.11 Access control
A.10 Cryptography	1	2	A.12.3 Cryptographic
A.11 Physical and environmental security	2	15	A.9 Physical and environmental
A.12 Operations security	7	14	A.10 Communications & Operations
A.13 Communications security	2	7	A.10 Communications & Operations
A.14 System acquisition, develop, maintain	3	13	A.12 acquisition, develop, maintain
A.15 Supplier relationships	2	5	A.6 External party /A.10.2 SD
A.16 info. Security incident management	1	7	A.13 incident management
A.17 Info, Security aspects of BCM	2	4	A.14 BCM
A.18 Compliance	2	8	A.15 Compliance
14	35	114	11/39/133

改版差異(附錄A)

ISO/IEC 27001:2005	Categories	Controls	ISO/IEC 27001:2013	Categories	Controls
A.5 Security policy	1	2	A.5 Security policy	1	2
A.6 Organization of information security	2	11	A.6 Organization of information security	2	7
A.7 Asset management	2	5	A.7 Human resources security	3	6
A.8 Human resources security	3	9	A.8 Asset management	3	10
A.9 Physical and environment security	2	13	A.9 Access control	4	13
A.10 Communications & operations management	10	32	A.10 Cryptography (New)	1	2
A.11 Access control	7	25	A.11 Physical and environment security	2	15
			A.12 Operations management	7	14
			A.13 Communications management	2	7
A.12 Information system acquisition, development and maintenance	6	16	A.14 System acquisition, development and maintenance	3	13
			A.15 Supplier relationships (New)	2	5
A.13 Information security incident management	2	5	A.16 Information security incident management	1	7
A.14 Business continuity management	1	5	A.17 Information security aspects of business continuity management	2	4
A.15 Compliance	3	10	A.18 Compliance	2	8
合計：11領域/39目標/133控制措施			合計：14領域/35目標/114控制措施		

ISO 27001:2013 控制目標概要



A.5 Information security policy
安全政策

ISO 27001:2013		
A.5.1	**Management direction for information security** **資訊安全管理方針**	
目標	依據營運需求和相關的法令法規，提供管理階層在資訊安全方針和支援	
A. 5.1.1	Policies for information security 資訊安全政策	一系列的資訊安全政策應該被管理階層定義和核准，並發佈和溝通與員工和相關外部團體
A. 5.1.2	Review of the policies for information security 資訊安全政策之審查	資訊安全政策應依規劃期間或重大變更時審查，已確保其持續的適用性、適切性及有效性

A.6 Organisation of information security
資訊安全的組織

ISO 27001:2013		
A.6.1	**Internal organisation 內部組織**	
目標	建立用於啟動與管制組織內資訊安全實作與運作的管理架構	
A.6.1.1	Information security roles and responsibilities 資訊安全角色與責任	所有資訊安全責任應加以界定與安排
A.6.1.2	Segregation of duties 職務的區隔 (A.10.1.3)	具有衝突性的職務與責任領域應加以區隔，已降低組織資產遭未經授權或非意圖的修改或誤用之機會
A.6.1.3	Contact with authorities 與權責機關的接觸	應與相關權責機關維持適當聯繫
A.6.1.4	Contact with special interest groups 與特殊利害相關團體的聯繫	應與個特殊利害相關團體或其他各種專家安全性論壇及專業協會維持適當聯繫

A.6 Organisation of information security
資訊安全的組織

ISO 27001:2013		
A.6.1.5	Information security in project management 專案計畫管理中的資訊安全	無論任何型態的專案，資訊安全都應在專案管理加以陳述
A.6.2	**Mobile devices and teleworking** **行動裝置與遠距工作**	
目標	確保遠距工作與行動設備使用的安全	
A.6.2.1	Mobile device policy 行動裝置政策	政策與支援性的安全措施應加以適用，以管理因使用行動設備而產生的風險
A.6.2.2	Teleworking 遠距工作	政策與支援性的安全措施應加以實作，以保護由遠距區域存取、處理與儲存的資訊

A.7 Human resources security
人力資源安全

ISO 27001:2013		
A.7.1	**Prior to employment 聘僱之前**	
目標	確保員工與承包者了解其責任，並勝任期所被認定的角色	
A.7.1.1	Screening 篩選	應比較相關法律、法規及倫理，並兼顧營運要求的比例原則、所存取資訊的機密類別及所察覺的風險，對所有聘僱之應徵者進行背景查證檢核
A.7.1.2	Terms and conditions of employment 聘僱條款與條件	與員工及契約人員的契約協議應陳述其與組織對資訊安全責任

A.7 Human resources security
人力資源安全

ISO 27001:2013		
A.7.2	**During employment 聘僱期間**	
A.7.2.1	Management responsibilities 管理階層責任	管理階層應要求員工與契約人員，依照組織已制定的政策與程序施行安全事宜
A.7.2.2	Information security awareness, education and training 資訊安全認知、教育及訓練	組織所有員工和相關的契約人員，均應接受與其工作職務相關之適切認知教育訓練，以及定期更新的組織政策與程序內容
A.7.2.3	Disciplinary process 懲處過程	應有正式並以溝通的懲處過程，來採取行動處理違反資訊安全的員工

A.7 Human resources security
人力資源安全

ISO 27001:2013		
A.7.3	**Termination and change of employment** **聘僱的終止或變更**	
目標	將保護組織的利益，視作在變更或終止職務的流程的一部分	
A.7.3.1	Termination or change of employment responsibilities 終止或變更責任	在聘僱終止或變更後持續有效的資訊安全責任與義務，應加以界定，並向員工與契約人員溝通與執行

A.8 Asset management
資產管理

ISO 27001:2013		
A.8.1	**Responsibility for assets** **資產責任**	
目標	識別組織資產，並界定適當的保護責任	
A.8.1.1	Inventory of assets 資產清冊	資訊與資訊處理設施相關的資產應加以識別，該資產清單應加以製作與維護
A.8.1.2	Ownership of assets 資產的擁有權	資產清冊中維護的資產應有擁有者
A.8.1.3	Acceptable use of assets 資產之可被接受的使用	資訊與資訊處理設施相關的資訊與資產，於可被接受的使用規則應予以識別、文件化及實作
A.8.1.4	Return of assets 資產的歸還	所有員工與外部團體使用在其聘僱、契約或協議終止時，應歸還其擁有的所有組織資產

A.8 Asset management
資產管理

ISO 27001:2013		
A.8.2	**Information classification** **資訊分類**	
目標	確保所有資產能依據對組織的重要性獲得適切程度的保護	
A.8.2.1	Classification of information 資訊分類	資訊應依其對未經授權的揭露或修改的法律要求、價值、重要性與敏感性加以分級
A.8.2.2	Labeling of information 資訊標示	應依照組織所採用的分類法，發展與實作一套適當的資訊標示程序
A.8.2.3	Handling of assets 資產處置	應依照組織所採用的分類法，發展與實作一套適當的資產處置程序

A.8 Asset management
資產管理

ISO 27001:2013		
A.8.3	**Media handling** **媒體的處置**	
目標	避免存放於媒體的資訊受到未經授權的揭露、修改、移除與破壞	
A.8.3.1	Management of removable media 可移除式媒體的管理	應依照組織所採用的分類法，實作可移除是媒體管理程序
A.8.3.2	Disposal of media 媒體的汰除	媒體不再需要時，應加以安全的汰除
A.8.3.3	Physical media transfer 輸送中的實體媒體	應保護含有資訊的媒體在傳輸時應被保護，避免未經授權的存取、誤用或毀損

A.9 Access control
存取控制

ISO 27001:2013		
A.9.1	**Business requirements of access control 存取控制的營運要求**	
目標	限制資訊與資訊處理設施的存取	
A.9.1.1	Access control policy 存取控制政策	應基於營運與資訊安全要求，建立、文件化及審查存取控制政策
A.9.1.2	Access to networks and network services 網路與網路服務存取	僅提供使用者經特定授權可存取的網路與網路服務
A.9.2	**User access management** **使用者存取管理**	
目標	確保授權使用者得以存取，並避免系統與服務的未授權存取	
A.9.2.1	User registration and de-registration 使用者註冊與註銷	正式的使用者註冊與註銷流程應加以實作，以確保存取權限的指派
A.9.2.2	User Access Provisioning 使用者存取提供	正式使用者存取提供流程應加以實作，以指派或撤銷所有系統與服務之各項使用者類別的存取權限

A.9 Access control
存取控制

ISO 27001:2013		
A.9.2.3	Management of privileged access right 特權管理	應限制與控制特權的配置與使用
A.9.2.4	Management of secret authentication information of users 使用者秘密授權資訊的管理	秘密授權資訊的配置應透過正式管理流程加以控制
A.9.2.5	Review of user access rights 使用者存取權限的審查	資產擁有者應定期審查使用者的存取權限
A.9.2.6	Removal or adjustment of access rights 存取權限的移除或調整	所有員工與外部團體使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除

A.9 Access control
存取控制

ISO 27001:2013		
A.9.3	**User responsibilities** **使用者責任**	
目標	讓使用者對保護其授權者資訊安全負起責任	
A.9.3.1	Use of secret authentication information 秘密授權資訊的使用	應要求使用者於使用秘密授權資訊時，遵循組織實務

A.9 Access control
存取控制

ISO 27001:2013		
A.9.4	**System and application access control** **系統與應用程式存取控制**	
目標	防止系統與應用程式的未授權存取	
A.9.4.1	Information access restriction 資訊存取限制	應根據存取控制政策，限制對資訊與應用系統功能之存取
A.9.4.2	Secure log-on procedures 保全登入程序	當有存取控制政策要求時，應由保全登入程序來控制系統與應用程式的存取
A.9.4.3	Password management system 通行碼管理系統	管理通行碼的系統應為互動式，並應確保通行碼嚴謹
A.9.4.4	Use of privileged utility programs 特權公用程式的使用	可能篡越系統與應用控制措施的公用程式之使用，應加以限制與嚴密控制
A.9.4.5	Access control to program source code 程式源碼的存取控制	應用程式原始碼的存取應加以限制

A.10 Cryptography
密碼控制

ISO 27001:2013		
A.10.1	**Cryptographic controls** **密碼控制措施**	
目標	確保適當有效地使用密碼措施，以保護資訊的機密性、鑒別性與/或完整性	
A.10.1.1	Policy on the use of cryptographic controls 使用密碼控制措施的政策	使用密碼控制措施以保護資訊的政策應加以發展與實作
A.10.1.2	Key management 金鑰管理	加密金鑰使用、保護與存續期間的政策，應加以發展與實作於整個生命週期

A.11 Physical and environmental security
實體與環境安全

ISO 27001:2013		
A.11.1	**Secure areas 安全區域**	
目標	防止組織資訊與資訊處理設施遭未經授權的實體存取、損害及干擾	
A.11.1.1	Physical security perimeter 實體安全周界	安全周界應加以界定與使用，以保護含有敏感或重要資訊及資訊處理設施的區域
A.11.1.2	Physical entry controls 實體進入控制措施	安全區域應藉由適當的入口控制措施加以保護，以確保只有經授權人員方可允許進出
A.11.1.3	Securing office, room and facilities 保全辦公室、房間及設施	應設計辦公室、房間及設施的實體安全並施行之
A.11.1.4	Protecting against external end environmental threats 對外部與環境威脅的保護	應設計並施行實體保護，以避免天然災害、惡意攻擊或意外

A.11 Physical and environmental security
實體與環境安全

ISO 27001:2013		
A.11.1.5	Working in secure areas 在安全區域內工作	安全區域內工作的程序應加以設計與施行
A.11.1.6	Delivery and loading areas 收發及裝卸區	諸如收發與裝卸區及其他未經授權人員可進入作業場所之進出點一加以控制；若可能，並宜與資訊處理設施隔離，以避免未經授權的存取
A.11.2	**Equipment 設備**	
目標	防止資產的遺失、損害、竊盜或破解，並防止組織作業的中斷	
A.11.2.1	Equipment siting and protection 設備安置與保護	應安置或保護設備，以降低來自環境之威脅與危害造成的風險，以及未經授權存取之機會
A.11.2.2	Supporting utilities 支援的公用設施	應保護設備不受電源失效及其他支援的公用設施失效所導致中斷的影響

A.11 Physical and environmental security
實體與環境安全

ISO 27001:2013		
A.11.2.3	Cabling security 佈纜的安全	應保護傳送資料或支援資訊服務之電源與電信佈纜，以防止竊聽、干擾或損害
A.11.2.4	Equipment maintenance 設備維護	應正確地維護設備，以確保其持續的可用性與完整性
A.11.2.5	Removal of assets 資產的攜出	未經事前授權，設備、資訊或軟體不應帶出場外
A.11.2.6	Security of equipment and assets off-premises 場所外設備與資產的安全	安全應適用於場外的設備，並考慮其在組織場所外工作的各種不同風險
A.11.2.7	Security disposal or re-use of equipment 設備的安全汰除或再使用	含有儲存媒體的設備，其所有項目在汰除前應加以檢核，以確保任何敏感性的資料與有版權的軟體已被移除或安全地覆寫

A.11 Physical and environmental security
實體與環境安全

ISO 27001:2013		
A.11.2.8	Unattended user equipment 無人看管的使用者設備	使用者應確保無人看管的設備有適當保護
A.11.2.9	Clear desk and clear screen policy 桌面淨空與螢幕淨空政策	應採用對紙本媒體與可移除式儲存媒體之桌面淨空政策，及資訊處理設施的螢幕淨空政策

A.12 Operations security
作業安全

ISO 27001:2013		
A.12.1	**Operational procedures and responsibilities** **作業之程序與責任**	
目標	確保正確與安全地操作資訊處理設施	
A.12.1.1	Documented operating procedures 文件化作業程序	作業程序應加以文件化，並讓所有需要的使用者均可隨時取得
A.12.1.2	Change management 變更管理	影響資訊安全的組織、營運流程、資訊處理設施與系統變更應加以控制
A.12.1.3	Capacity management 容量管理	各項資源的使用應加以監視、調協（tune)，並對未來容量要求預做規劃，以確保所要求的系統效能
A.12.1.4	Separation of development, testing and operational environments 開發、測試及運作環境的分隔	開發、測試及運作之環境應加以分隔，以降低對運作之環境未經授權存取或變更的風險

A.12 Operations security
作業安全

ISO 27001:2013		
A.12.1	**Protection from malware** **防範惡意程式**	
目標	確保資訊與資訊處理設施受到防範惡意碼的保護	
A.12.2.1	Controls against malware 對抗惡意碼的控制措施	防範惡意碼的偵測、預防及復原控制措施，應加以實作，並應結合適切的使用者認知
A.12.3	**Backup 備份**	
目標	防範資料損失	
A.12.3.1	Information backup 資訊備份	應依據所一定的備份政策，定期進行資訊、軟體與系統影像檔的備份與測試

A.12 Operations security
作業安全

ISO 27001:2013		
A.12.4	**Logging and monitoring** **存錄與監視**	
目標	紀錄事件與產生證據	
A.12.4.1	Event logging 事件存錄	事件存錄係記錄使用者活動、例外情形、錯誤及資訊安全事件，應加以產生、保存並定期審查
A.12.4.2	Protection of log information 日誌資訊的保護	存錄設施與日誌資訊應加以保護，以避免竄改與未經授權的處理
A.12.4.3	Administrator and operator logs 管理者與操作者日誌	系統管理者與操作者的活動應加以存錄、保護及定期審查
A.12.4.4	Clock synchronisaon 鐘訊同步	組織或安全領域內所有相關資訊處理系統的鐘訊，應與單一參考時間來源同步

A.12 Operations security
作業安全

ISO 27001:2013		
A.12.5	**Control of operational software** **作業軟體的控制**	
目標	確保作業系統上的軟體安裝	
A.12.5.1	Installation of software on operational systems 作業系統上軟體的安裝	應實作程序來控制作業系統上的軟體安裝
A.12.6	**Technical vulnerability management** **技術脆弱性管理**	
目標	防止技術脆弱性被利用	
A.12.6.1	Management of technical vulnerabilities 技術脆弱性的管理	應及時取得關於使用中資訊系統的技術脆弱性資訊、評估組織對此等脆弱性的暴露，以及採取適當的措施以因應相關風險
A.12.6.2	Restrictions on software installation 安裝軟體的限制	使用者軟體安裝的管理規則應加以建立與實作

A.12 Operations security
作業安全

ISO 27001:2013		
A.12.7	**Information systems audit considerations** **資訊安全稽核**	
目標	將稽核活動對作業系統的影響降至最低	
A.12.7.1	Information systems audit controls 資訊系統稽核控制	有關作業系統查核的稽核要求與活動，應謹慎規劃及議定，使營運過程中斷之風險降至最低

A.13 Communications security
通訊安全

ISO 27001:2013		
A.13.1	**Network security management網路安全管理**	
目標	確保網路與其支援資訊處理設施上的資訊的保護	
A.13.1.1	Network controls 網路控制措施	網路應適切地加以管理與控制，以保護系統與應用
A.13.1.2	Security of network services 網路服務的安全	所有網路服務的安全機制、服務水準及管理要求，應加以識別並納入網路服務協議中，不論此等服務是由內部或委外所提供
A.13.1.3	Segregation in networks 網路區隔	資訊服務、使用者及資訊系統等各群組使用的網路應加以區隔

A.13 Communications security
通訊安全

ISO 27001:2013		
A.13.2	**Information transfer** **資訊傳遞**	
目標	維護組織內及與任何外部單位資訊傳遞的安全	
A.13.2.1	Information transfer policies and procedures 資訊傳遞政策與程序	應備妥適當的正式傳遞政策、程序及控制措施，以保護資訊傳遞中所使用所有形式的通訊設施
A.13.2.2	Agreements on information transfer 資訊傳遞協議	組織與外部團體間的協議應說明營運資訊傳遞的安全
A.13.2.3	Electronic messaging 電子傳訊	電子傳訊涉及的資訊應被適當地加以保護
A.13.2.4	Confidentiality or non-disclosure agreements 機密或保密協議	反映組織對資訊保護之需求的機密性或保密協議要求，應加以識別、定期審查與文件化

A.14 System acquisition, development and maintenance資訊系統取得、開發與維護

ISO 27001:2013		
A.14.1	**Security requirements of information systems** **資訊系統的安全要求**	
目標	確保資訊安全是整體資訊系統生命週期的一部分，這也包含透過公共網路提供服務的資訊系統之安全要求	
A. 14.1.1	Information Security requirements analysis and specification 資訊安全需求分析與規格	資訊安全相關需求應包含於新資訊系統或現有資訊系統提昇的要求事項中
A. 14.1.2	Securing applications services on public networks 公共網路上的應用服務安全	公眾網路上傳輸而涉及應用服務的資訊，應加以保護免於詐欺行為、契約爭議及未經授權的揭露與修改
A. 14.1.3	Protecting application services transactions 保護應用服務交易	涉及應用服務交易的資訊，應加以保護以防止不完整的傳輸、錯誤路由（mis-routing)，以及未經授權的訊息修改、揭露、訊息複製或重演

A.14 System acquisition, development and maintenance資訊系統取得、開發與維護

ISO 27001:2013		
A.14.2	**Security in development and support processes** **開發與支援過程的安全**	
目標		
A. 14.2.1	Secure development policy 安全開發政策	軟體與系統開發規則應加以建立與應用於組織的系統開發中
A. 14.2.2	System change control procedures 系統變更控制程序	系統開發生命週期中的變更，應使用正式變更控制程序加以控制
A. 14.2.3	Technical review of applications after operating platform changes 作業系統平台變更後的應用系統技術審查	作業平台變更時，營運關鍵應用系統應加以審查與測試，以確保對組織作業或安全無不利的衝擊
A. 14.2.4	Restrictions on changes to software packages 套裝軟體變更的限制	應不鼓勵套裝軟體之修改，僅限於必要的變更，且所有的變更應被嚴格管制

A.14 System acquisition, development and maintenance資訊系統取得、開發與維護

ISO 27001:2013		
A. 14.2.5	Secure system engineering principles 安全系統設計原則	設計安全系統的原則應加以建立、文件化、維護並應用於所有資訊系統實作成果
A. 14.2.6	Secure development environment 安全開發環境	組織應建立且適切的保護涵蓋整個系統開發生命週期中針對系統開發和整合活動時的安全開發環境
A. 14.2.7	Outsourced development 委外開發	組織應監督與監視委外系統開發的活動
A. 14.2.8	System security testing 系統安全測試	安全功能的測試應於開發中執行
A. 14.2.9	System acceptance testing 系統驗收測試	新資訊系統、升級及新版本的驗收測試方案與相關準則應被建立

A.14 System acquisition, development and maintenance資訊系統取得、開發與維護

ISO 27001:2013		
A.14.3	**Test data** **測試資料**	
目標	確保用於測試的資料受到保護	
A. 14.3.1	Protection of test data 測試資料的保護	測試資料應加以小心選擇、保護及管制

A.15 Supplier relationships
供應商關係

ISO 27001:2013		
A.15.1	**Information security in supplier relationships** **供應商關係中的資訊安全**	
目標	確保供應商可存取的組織資產受到保護	
A. 15.1.1	Information security policy for supplier relationships 供應商關係的資訊安全政策	為降低供應商存取組織資產相關風險的資訊安全要求事項資訊，應取得供應商的同意並加以文件化
A. 15.1.2	Addressing security within supplier agreements 供應商協議的安全說明	所有相關的資訊安全要求事項，均應被建立並取得涉及存取、處理、儲存、溝通或提供IT基礎設施元件供應商的同意
A. 15.1.3	Information and communication technology (ICT) supply chain 資通訊技術供應鏈	供應商協議應包含說明資訊與通信技術服務與產品供應鏈有關的資訊安全風險

A.15 Supplier relationships
供應商關係

ISO 27001:2013		
A.15.2	**Supplier service delivery management** **供應商服務交付管理**	
目錄	維持適切等級之資訊安全及服務交付，並能與供應商協議一致	
A. 15.2.1	Monitoring and review of supplier services 供應商服務的監視與審查	組織應定期監視、審查與稽核供應商的服務交付
A. 15.2.2	Managing changes to supplier services 供應商服務變更的管理	供應商所提供服務的變更，包括維持與改進現有的資訊安全政策、程序及控制措施均應加以管理，並考量所涉及之營運系統與過程的重要性以及風險的重新評鑑

A.16 Information security incident management 資訊安全事故管理

ISO 27001:2013		
A.16.1	**Management of information security incidents and improvements** **資訊安全事故與改善**	
目錄	確保包含資安事件與弱點溝通的資訊安全事故管理採用一致與有效的作法	
A.16.1.1	Responsibilities and procedures 責任與程序	管理責任與程序應加以建立，以確保對資訊安全事故作迅速、有效及依序的回應
A.16.1.2	Reporting information security events 通報資訊安全事件	資訊安全事件應詢適切的管理管道儘速通報
A.16.1.3	Reporting information security weaknesses 通報資訊安全弱點	使用組織資訊系統與服務的所有員工與契約人員，應被要求注意並通報系統或服務之任何觀察到或可疑的安全弱點

A.16 Information security incident management 資訊安全事故管理

ISO 27001:2013		
A. 16.1.4	Assessment and decision of information security events 資訊安全事件的評估與決策	資訊安全事件應加以評估與決策其是否應歸類為資訊安全事故
A. 16.1.5	Response to information security incidents 資訊安全事故的回應	資訊安全事故應依據文件化程序加以回應
A. 16.1.6	Learning from information security incidents 從資訊安全事故中學習	由分析與解決資訊安全事故所獲得的知識，應利用來降低未來事故發生可能性與衝擊性
A. 16.1.7	Collection of evidence 證據的收集	組織硬制定並應用程序來進行可作為證據資訊的識別、蒐集、取得與保存

A.17 Information security aspects of business continuity management營運持續管理的資訊安全層面

ISO 27001:2013		
A.17.1	**Information security continuity** **資訊安全持續性**	
目標	資訊安全持續性應鑲嵌於組織營運持續管理	
A.17.1.1	Planning information security continuity 規劃資訊安全持續性	組織應決定資訊安全與資訊安全管理在危急情況，如危機或災害期間的持續性要求
A.17.1.2	Implementing information security continuity 實作資訊安全持續性	組織應建立、文件話、實作與維護流程、程序與控制措施，以保障資訊安全在危急情況時達成所要求的持續性等級
A.17.1.3	Verify, review and evaluate information security continuity 驗證與審查資訊安全持續管理	組織應定期查核已建立與實作的資訊安全持續性控制措施，以確保其在危急情況的可用與有效性

A.17 Information security aspects of business continuity management營運持續管理的資訊安全層面

ISO 27001:2013		
A.17.2	**Redundancies** **備援（複式措施）**	
目標	確保資訊處理設施的可用性	
A.17.2.1	Availability of information processing facilities 資訊處理設施的可用性	資訊處理設施以備援（複式措施）來實作，以充分符合可用性要求

A.18 Compliance
遵循性

ISO 27001:2013		
A.18.1	**Compliance with legal and contractual requirements** **遵循適法性要求**	
目標	避免違反任何資訊安全相關法律、法令、法規或契約義務，以及任何安全要求	
A. 18.1.1	Identification of applicable legislation and contractual requirements 識別適用之法條與契約要求	對每個資訊系統與組織，所有相關法律、法令、法規、契約要求與組織用以符合這些要求的作法，均應加以明確界定、文件化及維持最新
A. 18.1.2	Intellectual property rights (IPR) 智慧財產權	適當程序應加以實作以確保遵循智慧財產權與所使用的專屬軟體產品的相關法律、法規及契約要求

A.18 Compliance
遵循性

ISO 27001:2013		
A. 18.1.3	Protection of records 記錄的保護	記錄應依據法令、法規、契約及營運要求，加以保護，以免於遺失、毀損、偽造、未授權存取與未授權發行
A. 18.1.4	Privacy and protection of personally identifiable information 個人識別資訊的隱私與保護	個人識別資訊的隱私與保護應加以確保符合相關適用法令法規的要求
A. 18.1.5	Regulation of cryptographic controls 密碼控制措施的規定	密碼控制措施的使用應遵循所有相關的協議、法律及法規

A.18 Compliance
遵循性

ISO 27001:2013		
A.18.2	**Information security reviews** **資訊安全審查**	
目標	確保資訊安全依據組織的政策與程序進行實作與運作	
A. 18.2.1	Independent review of information security 資訊安全的獨立審查	組織對管理資訊安全的作法與實作（例如：資訊安全的各項控制目標、控制措施、政策、過程及程序），應一所規劃的期間或當安全實作發生顯著變更時，進行獨立審查
A. 18.2.2	Compliance with security policies and standards 安全政策與標準的遵循性	管理者應定期審查其適當的資訊安全政策、標準與其他安全要求責任範圍內資訊處理與程序的遵循性
A. 18.2.3	Technical compliance review 技術遵循性審查	資訊系統應定期審查組織資訊安全政策與標準的遵循性

新增的控制項目

- A.6.1.1 Information security roles and responsibilities資訊安全角色與責任
- A.6.1.4 Information security in project management專案計畫管理中的資訊安全
- A.6.2.1 Mobile device policy行動裝置政策
- A.8.2.3 Handling of assets資產的處置
- A.9.2.3 Management of secret authentication information of users使用者鑑別資訊的管理
- A.9.3.1 Use of secret authentication information鑑別資訊的使用
- A.12.5.1 Installation of software on operational systems作業系統上軟體的安裝
- A.12.6.2 Restrictions on software installation安裝軟體的限制

新增的控制項目

- A.14.1.2 Securing applications services on public networks公開網路上的應用服務安全
- A.14.1.3 Protecting application services transactions保護應用服務變更
- A.14.2.1 Secure development policy安全開發政策
- A.14.2.5 System development procedures系統開發程序
- A.14.2.6 Secure development environment安全開發環境
- A.14.2.8 System security testing系統安全測試
- A.14.2.9 System acceptance testing系統驗收測試
- A.15.1.1 Information security policy for supplier relationships供應商關係的安全資訊政策
- A.15.1.3 ICT supply chain

新增的控制項目

- A.16.1.4 Assessment and decision of information security events資訊安全事件的評估與判斷
- A.16.1.5 Response to information security incidents資訊安全事故通報
- A.17.1.1 Planning information security continuity規劃資訊安全持續管理
- A.17.1.2 Implementing information security continuity實作資訊安全持續管理
- A.17.1.3 Verify, review and evaluate information security continuity驗證與審查資訊安全持續管理
- A.17.2 Redundancies備援
- A.17.2.1 Availability of information processing facilities資訊設備的可用性


Q & A……