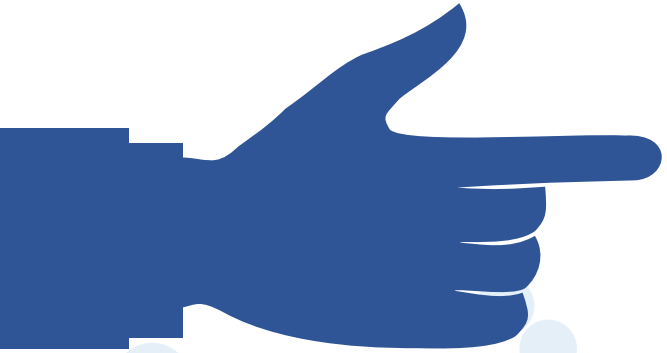
ISO/IEC 27001 : 2022

資訊安全，網路安全及隱私保護

- 資訊安全管理系統轉版課程



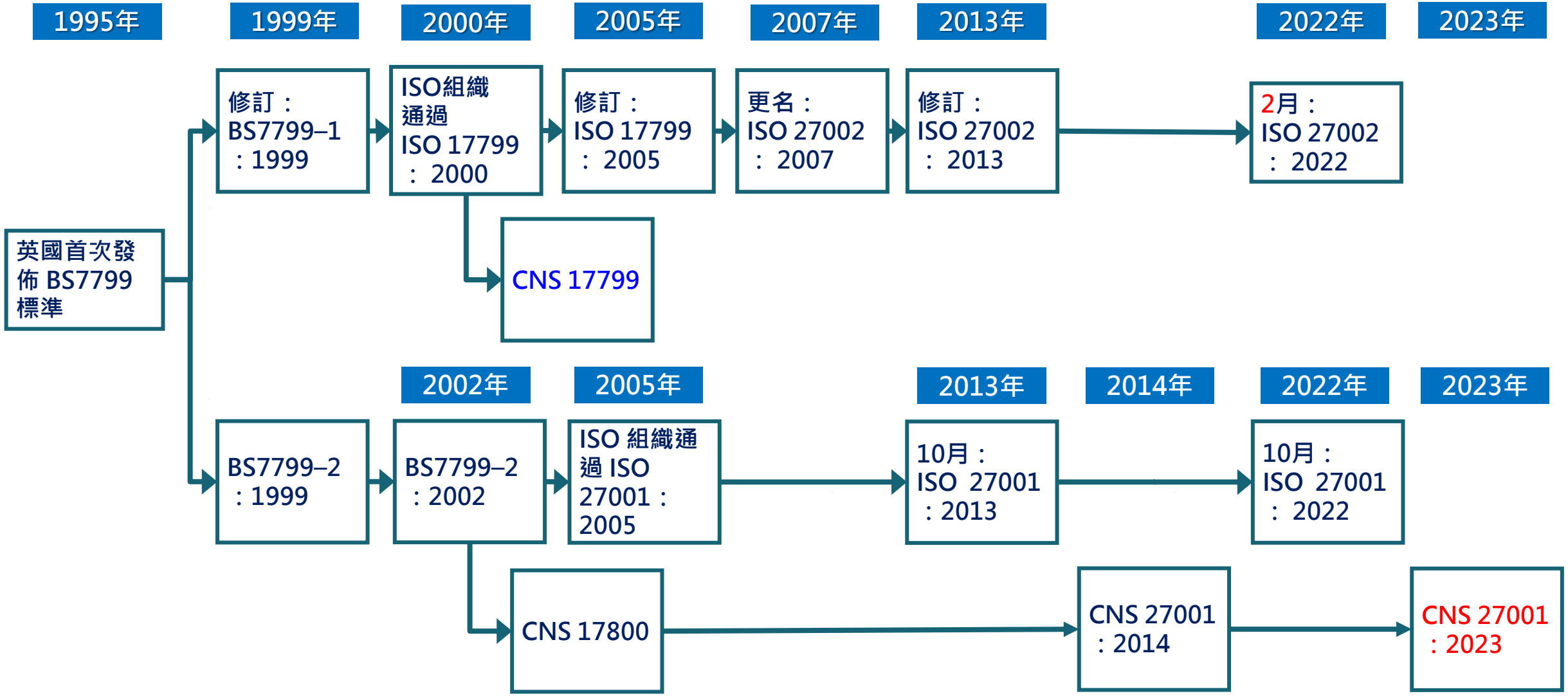
中華民國 113 年 09 月 04 日

課程大綱

- ISMS標準發展與修訂背景
- 新舊版標準關鍵差異分析
- 新版標準條文理解與運用
- 新版標準 附錄A 安全控制措施之詮釋與運用

標準發展與修訂背景

- ISO / IEC 27001資訊安全管理制度發展歷程



課程大綱

- ISMS標準發展與修訂背景
- 新舊版標準關鍵差異分析
- 新版標準條文理解與運用
- 新版標準 附錄A 安全控制措施之詮釋與運用

新舊版標準關鍵差異分析

如何改變

- 主條文差異
- 附錄A-控制措施的改變

主條文差異　ISO 27001：2022

1.名稱 → 2.頁數與方向 → 3.術語與定義（參考資訊） → 4.新增要求（4.2瞭解利害關係方的需求與期望）

5. 強化過程導向（4.4資訊安全管理系統） → 6. 新增要求（6.2資訊安全目標與達成之規劃） → 7. 新增要求（6.3變更規劃） → 8. 簡化要求（7.4溝通）

9. 新增要求（8.1 運作的規劃與控管） → 10. 新增要求（9.1 監督、量測、分析與評估） → 11. 要求架構變更（9.2、9.3） → 12.要求架構變更（10.改善）

1. 名稱

ISO 27001：2013

ISO/IEC 27001:2013

Information technology — Security techniques — Information security management systems — Requirements

資訊技術 - 安全技術 - 資訊安全管理系統 - 要求事項

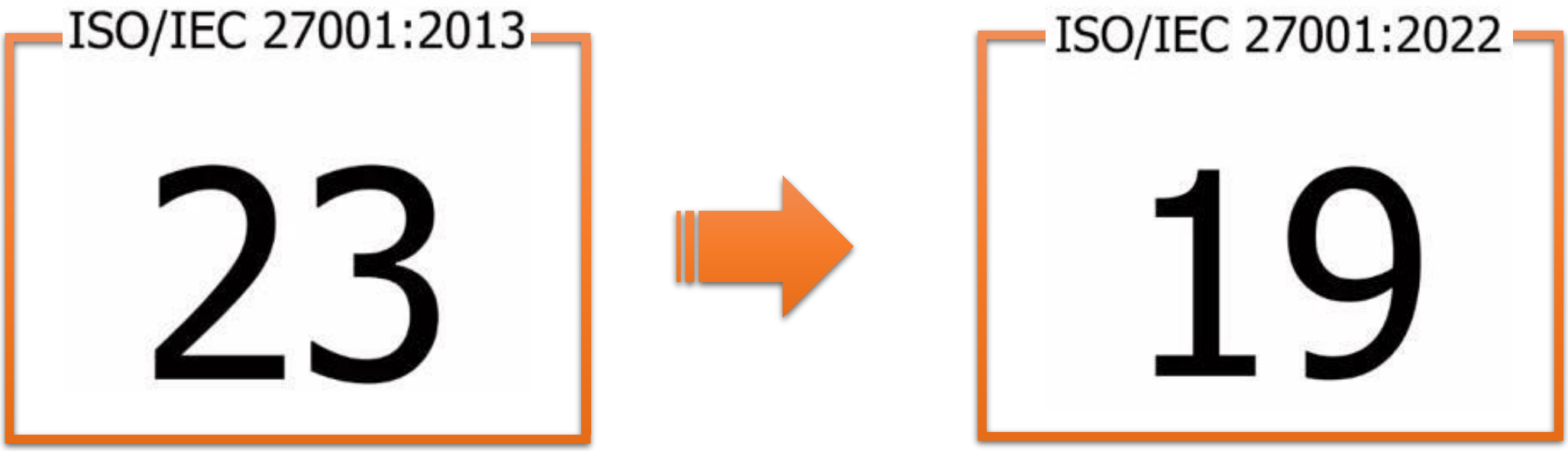
ISO 27001：2022

ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

資訊安全 - 網路安全與隱私保護 - 資訊安全管理系統 - 要求事項

2. 頁數與方向



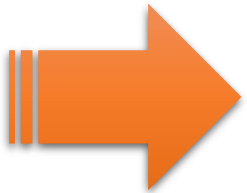
- 以「文件 (Document)」全數取代「國際標準 (International Standard)」。
- 重新編排子編號的結構，使能與調和方法保持一致。
- 重新編排部份英文內容，以更利於翻譯。

3. 術語與定義（參考資訊）

ISO/IEC 27001:2013

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.



ISO/IEC 27001:2022

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp
— IEC Electropedia: available at https://www.electropedia.org

4. 新增要求（4.2 瞭解利害關係者的需求和期望）

ISO 27001：2013

4.2 了解利害關係者的需求與期望

組織應決定：

a) 與ISMS有關的利害關係者；以及

b) 這些利害關係者對資訊安全之要求。

備註：這些利害關係者的要求可能包含了法規要求與契約義務。

ISO 27001：2022

4.2 瞭解利害關係者的需求和期望

組織應決定：

a) 與資訊安全管理系統相關的利害關係者；

b) 利害關係者的相關要求事項；

c) 此等要求事項中之哪些要求事項將透過資訊安全管理系統因應。

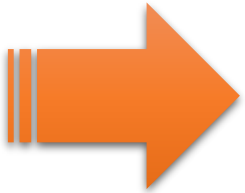
備註：利害關係者之要求事項可以包括法令要求事項及契約義務。

5. 強化過程導向（4.4 資訊安全管理系統）

ISO 27001：2013

4.4 資訊安全管理系統

組織應依據本標準的要求，以建立、實施、維護和持續改進ISMS。



ISO 27001：2022

4.4 資訊安全管理系統

組織應依**本文件**之要求事項，建立、實施、維持及持續改善資訊安全管理系統，**包括所需過程及其互動**。

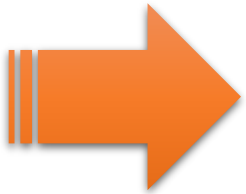
6. 新增要求（6.2 資訊安全目標與達成之規劃）

ISO 27001：2013

6.2 資訊安全目標與達成之規劃

組織應在相關的功能與層級中建立資訊安全目標。

資訊安全目標應：
a) 與資訊安全政策一致；
b) 可測量（如果可行時）；
c) 考量適用的資訊安全要求，以及風險評鑑與處理結果；
a) 經過溝通，且
b) 適當時作更新。



ISO 27001：2022

6.2 資訊安全目標與達成之規劃

組織應於各相關部門及層級建立資訊安全目標。

資訊安全目標應滿足下列事項：
a) 與資訊安全政策一致。
b) 可測量（若可行時）。
c) 考量適用之資訊安全要求，以及風險評鑑與風險處理的結果。
d) 受到監控。
e) 經過溝通。
f) 適當時作更新。
g) 以文件化資訊提供。

7. 新增要求（6.3 變更之規劃）

6.3 變更之規劃

當組織決定需要對資訊安全管理系統變更時，應以規劃之方式執行變更。

ISO 27001：2013 無此項要求

When the organization determines the need for changes to the information security management system, the changes shall be carried out **in a planned manner**

8. 簡化要求（7.4 溝通）

ISO 27001：2013

7.4 溝通

組織應決定與ISMS有關的內部與外部溝通之需求，包含：

a) 溝通什麼；
b) 何時溝通；
c) 和誰溝通；
d) 誰應溝通；以及
e) 應實現哪種溝通過程。

ISO 27001：2022

7.4 溝通

組織應決定，相關於資訊安全管理系統之內部及外部溝通或傳達的需要，包括下列事項：

a) 溝通什麼。
b) 何時溝通。
c) 和誰溝通。
d) 如何溝通。

9. 新增要求（8.1 運作之規劃及管控）

ISO 27001：2013

8.1 運作的規劃與控管

組織應規劃、實施與控管可符合資訊安全要求，及實施在條文 6.1 所決定的行動。組織也應實施計畫，以達成在條文6.2 所決定的資訊安全目標。

組織應依照計畫實現過程所必需的信心程度，保存文件化資訊。

組織應管制計畫的變更，並審查無預期的變更會帶來的後果，在必要時，採取措施以減輕任何不良影響。

組織應確認委外之過程是被建立及控管。

ISO 27001：2022

8.1 運作之規劃及管控

組織應規劃、實施及控制符合要求事項所需之過程，並藉由下列方式，實作條文6中所決定的行動。

- **建立過程之準則；**
- **依準則實作過程之控制措施。**

文件化資訊應在必要的程度上提供可用來確認過程已按計劃進行。

組織應控制所規劃之變更，並審查非預期變更的後果，必要時採取行動以減輕任何不利影響。

組織應確保有關資訊安全管理系統之外部提供的過程、產品或服務受到控制。

10. 新增要求（9.1 監督、量測、分析和評估）

ISO 27001：2013

9.1 監督、量測、分析與評估

組織應評估資訊安全的績效與ISMS的有效性，並決定：.....

組織應保存適當的文件化資訊，以作為監督與量測結果的證據。

ISO 27001：2022

9.1 監督、量測、分析和評估

組織應決定下列事項：.....

文件化資訊應是可用的，以作為結果的證據。

組織應評估資訊安全管理系統之資訊安全績效及有效性。

11. 要求架構變更（9.2、9.3）

ISO 27001：2013

9.2 內部稽核

9.3 管理階層審查

ISO 27001：2022

9.2 內部稽核

- 9.2.1 一般要求
- 9.2.2 內部稽核方案

9.3 管理審查

- 9.3.1 一般要求
- 9.3.2 管理審查輸入事項
- 9.3.3 管理審查結果

新增輸入事項：c) 與資訊安全管理相關的關注方的需求和期望的變化

12. 要求架構變更（10.改善）

ISO 27001：2013	ISO 27001：2022
10.1 不符合事項與矯正措施	10.1 持續改善
10.2 持續改善	10.2 不符合項目與矯正措施

附錄A - 控制措施的改變

如何改變

- 整體架構
- 控制措施屬性
- 控制措施內容架構

1. 整體架構

ISO 27001：2013

系統框架

- A.5 安全政策
- A.6 資訊安全組織
- A.7 人力安全管理
- A.8 資產管理

管控作業

- A.10 密碼技術
- A.11 實體及環境之安全管理
- A.12&13 作業與通訊管理
- A.14 資訊系統之獲得、發展和維修
- A.15 供應商管理
- A.9 存取控制

未來風險

- A.16 資訊安全事件之處理
- A.17 商業營運持續管理

- A.18 承諾與遵循

總計：114項控制措施

ISO 27001：2022

- A.5 組織面 控制措施 Total：37 保留34 / 新增3項
- A.6 人員面 控制措施 Total： 8項皆屬既有
- A.7 實體面 控制措施 Total：14 保留13 / 新增1項
- A.8 技術面 控制措施 Total：34 保留27 / 新增7項

總計：93項控制措施 (82+新增11項)

2. 控制措施屬性

01 控制措施種類

用於從控制措施**何時以及如何修改**與資訊安全事故發生的**相關風險**之觀點來檢視控制措施。屬性值包括預防性、偵測性和矯正性。

02 資訊安全特性

用於從控制措施將**有助於保留資訊的哪些特徵**之觀點來檢視控制措施。屬性值包括機密性、完整性和可用性。

03 網路安全概念

網路安全概念是從與ISO / IEC TS 27110中描述之網路安全框架中定義的**網路安全概念之控制措施**所關聯的觀點來檢視控制措施的屬性。**屬性值包括識別、保護、偵測、回應和復原。**

04 運作能力

運作能力是從**資訊安全能力的實踐者**觀點來檢視控制措施的一個屬性。

屬性值包括治理、資產管理、資訊保護、人力資源安全、實體安全、系統與網路安全、應用程式安全、安全組態、身份與存取管理、威脅與弱點管理、持續性、供應商關係的安全、適法與遵循性、資訊安全事件管理和資訊安全保障。

05 安全領域

安全領域是從四個**資訊安全領域**的觀點來檢視控制措施的屬性，屬性值包括治理與生態系統、保護、防禦與復原力。

2. 控制措施屬性 - 範例

5 組織面控制措施

5.1 資訊安全政策

控制措施種類	資訊安全特性	網路安全概念	運作能力	安全領域
#預防性	#機密性 #完整性 #可用性	#識別	#治理	#治理與生態系統 #復原力

5.2 資訊安全的角色與職責

控制措施種類	資訊安全特性	網路安全概念	運作能力	安全領域
#預防性	#機密性 #完整性 #可用性	#識別	#治理	#治理與生態系統 #保護 #復原力

3. 控制措施內容架構

ISO 27002：2013

6.1.3 與權責機關之聯繫

控制措施
宜維持與相關權責機關之適切聯繫

實作指引
組織宜備妥程序，規定宜聯繫權責機關（例：執法單位、監理機關及主管機關）之時機及人員，以及已識別之資訊安全事故，宜如何已及時方式通報（例：若有違法疑慮）

其他資訊
可能受網際網路攻擊之組織，可能需權責機關採取作為以抵禦攻擊源。

維護此等聯繫可能係支援資訊安全事故管理（參照第16節）或營運持續及應變規劃過程（參照第17節）之要求事項。與監理機關之聯繫，對組織必須實作之法律或法規即將變更的預測及準備亦有助益。與其他權責機關之聯繫，包括公用事業（utility）、緊急服務、電力公司及醫療衛生與安全，例：消防部門（與營運持續有關）、電信業（與線路選路及可用性有關）、水公司
（與設備冷卻設施有關）等。

ISO 27002：2022

5.5 與權責機關的聯繫

控制措施種類	資訊安全特性	網路安全概念	運作能力	安全領域
#預防性 #矯正性	#機密性 #完整性 #可用性	#識別 #保護 #回應 #復原	#治理	#防禦 #復原力

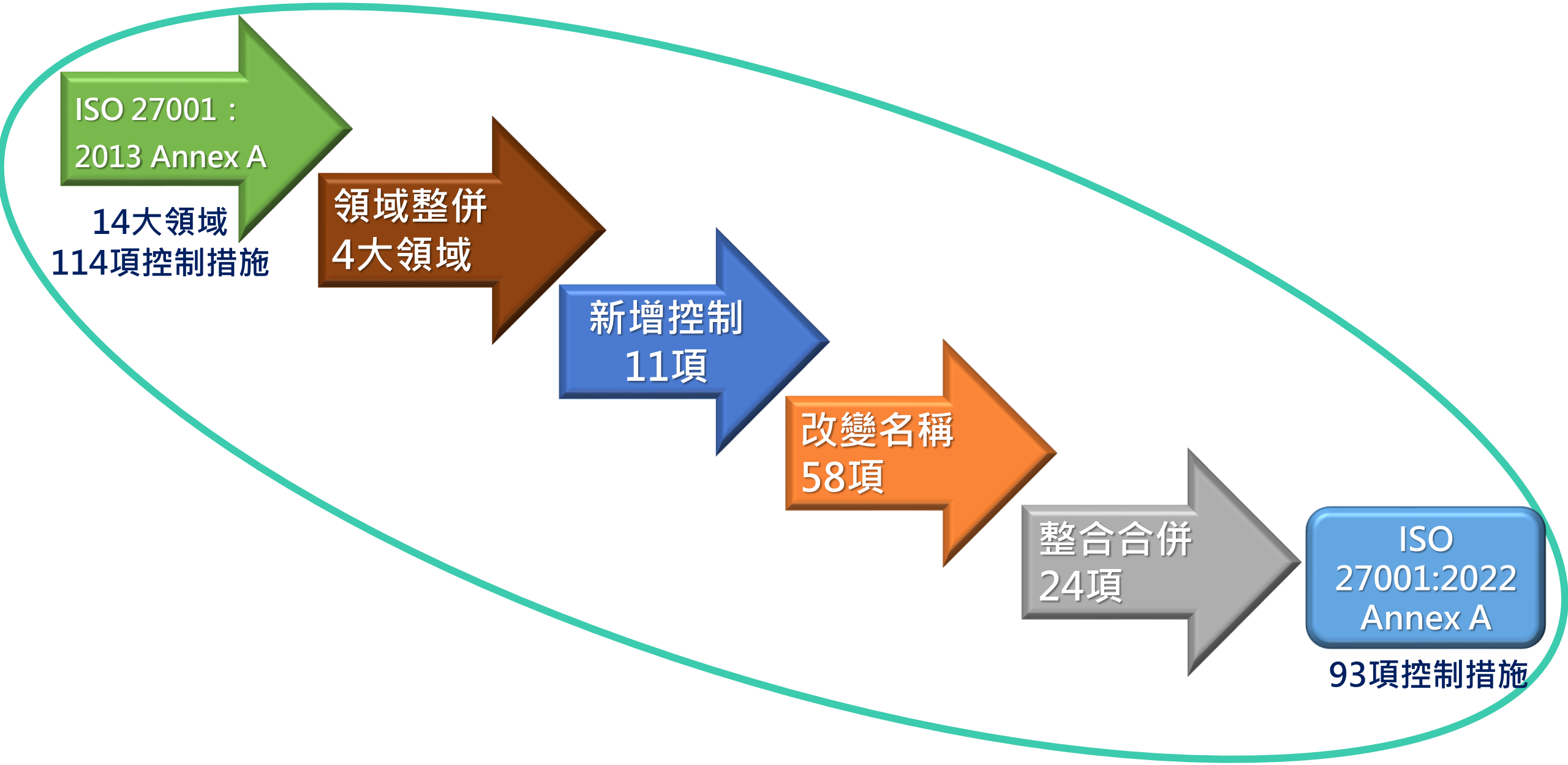
控制措施
組織應與有關之權責機關建立並保持聯繫。

目的
確保組織與相關法律、監管和監督機構之間在資訊安全方面進行適當的資訊流通。

指引
組織應指定何時和由誰聯繫權責機關（例如執法、監管機構、監督機構），以及如何及時報告已識別的資訊安全事件。
並且，應透過與權責機關的聯繫來促進了解這些權責機關當前和未來的期望（例如適用的資訊安全法規）。

其他資訊
受到攻擊的組織可以請求權責機關對攻擊來源採取行動。
保持此類聯繫可能是支援資訊安全事件管理的必要條件（見 5.24 至 5.28 ）或應變計劃和營運連續性之過程（見 5.29 和 5.30 ）。與監管機構的聯繫也有助於預測和準備即將發生之影響組織的相關法律或法規變化。與其他權責機關的聯繫包括公用事業、緊急服務、電力供應商以及健康和安全[例如消防部門（與營運連續性有關）、電信提供商（與線路路由和可用性有關）和供水商（與設備冷卻設施有關）]。

3. 控制領域與措施數量


ISO 27001：
2013 Annex A
14大領域
114項控制措施
領域整併
4大領域
新增控制
11項
改變名稱
58項
整合合併
24項
ISO
27001:2022
Annex A
93項控制措施

3. 控制措施數量（新增11項）

5.7	威脅情資
5.23	使用雲端服務之資訊安全
5.30	為營運持續性做好資通技術（ICT）的準備
7.4	實體安全監視
8.9	組態管理
8.10	資訊刪除
8.11	資料遮蔽
8.12	預防資料洩漏
8.16	活動監測
8.23	網頁過濾
8.28	安全編碼

3. 整併的控制措施數量（24項）

- 將有密切關連性或不可分割的原有捶制措施加以整併。

2013	2022	項目名稱
5.1.1、5.1.2	5.1	資訊安全政策
6.1.5、14.1.1	5.8	專案管理的資訊安全
8.1.1、8.1.2	5.9	資訊和其它相關資產的清冊
8.1.3、8.2.3	5.10	資訊和其它相關資產之可被接受的使用
13.2.1、13.2.2、13.3.3	5.14	資訊傳輸
9.1.1、9.1.2	5.15	存取控制
9.2.4、9.3.1、9.4.3	5.17	驗證資訊
9.2.2、9.2.5、9.2.6	5.18	存取權限
15.1.1、15.1.2	5.22	供應商服務之監控、審查及變更管理
17.1.1、17.1.2、17.1.3	5.29	中斷期間的資訊安全
18.1.1、18.1.5	5.31	法律、法令、法規及契約要求
18.2.2、18.2.3	5.36	資訊安全政策、規則與標準之遵循性

2013	2022	項目名稱
16.1.2、16.1.3	6.8	資訊安全事件通報
11.1.2、11.1.6	7.2	實體進出管制
8.3.1、8.3.2、8.3.3、11.2.5	7.10	儲存媒體
6.2.1、11.2.8	8.1	使用者終端裝置
12.6.1、18.2.3	8.8	技術漏洞的管理
12.4.1、12.4.2、12.4.3	8.15	日誌存錄
12.5.1、12.6.2	8.19	運作中系統上的軟體安裝
10.1.1、10.1.2	8.24	密碼學的使用
14.1.2、14.1.3	8.26	應用程式安全要求
14.2.8、14.2.9	8.29	開發與驗收的安全測試
12.1.4、14.2.6	8.31	區隔開發、測試與正式環境
12.1.2、14.2.2、14.2.3、14.2.4	8.32	變更管理

3. 更新控制措施描述（58項）1/2

2013	2022	項目名稱
6.1.1	5.2	資訊安全的角色與職責
6.1.2	5.3	職務區隔
7.2.1	5.4	管理階層責任
6.1.3	5.5	與權責機關的聯繫
6.1.4	5.6	與特殊利害關係者的聯繫
8.1.4	5.11	資產歸還
8.2.1	5.12	資訊分類
8.2.2	5.13	資訊標示
9.2.1	5.16	身份管理
15.1.1	5.19	供應商關係的資訊安全
15.1.2	5.20	供應商協議內的資訊安全要求
15.1.3	5.21	管理資通技術 (ICT) 供應鏈的資訊安全
16.1.1	5.24	資訊安全事故管理規劃與準備
16.1.4	5.25	資訊安全事件的評定與決策

2013	2022	項目名稱
16.1.5	5.26	對資訊安全事故的回應
16.1.6	5.27	從資訊安全事故中學習
16.1.7	5.28	證據的蒐集
18.1.2	5.32	智慧財產權
18.1.3	5.33	紀錄之保護
18.1.4	5.34	隱私與個人可識別資訊(PII)的保護
18.2.1	5.35	資訊安全之獨立審查
12.1.1	5.37	文件化的作業程序
7.1.1	6.1	篩選
7.1.2	6.2	聘僱條款與條件
7.2.2	6.3	資訊安全認知、教育與培訓
7.2.3	6.4	懲處程序
7.3.1	6.5	聘僱終止或變更後之責任
13.2.4	6.6	機密性或保密協議

3. 更新控制措施描述（58項）2/2

2013	2022	項目名稱
6.2.2	6.7	遠距工作
11.1.1	7.1	實體安全邊界
11.1.3	7.3	辦公室、空間與設施的保護
11.1.4	7.5	對抗實體與環境威脅的保護
11.1.5	7.6	在安全區域內工作
11.2.9	7.7	桌面淨空及螢幕淨空
11.2.1	7.8	設備安置與保護
11.2.6	7.9	場所外資產的安全
11.2.2	7.11	支援之公用設施
11.2.3	7.12	佈纜之安全
11.2.4	7.13	設備維護
11.2.7	7.14	設備汰除或再使用之安全
9.2.3	8.2	特殊存取權限
9.4.1	8.3	資訊存取限制
9.4.5	8.4	程式源碼的存取

2013	2022	項目名稱
9.4.2	8.5	安全驗證
12.1.3	8.6	容量管理
12.2.1	8.7	防範惡意程式
12.3.1	8.13	資訊備份
17.2.1	8.14	資訊處理設施的備援
12.4.4	8.17	時脈同步
9.4.4	8.18	特權的公用程式之使用
13.1.1	8.20	網路安全
13.1.2	8.21	網路服務的安全
13.1.3	8.22	網路區隔
14.2.1	8.25	安全之開發生命週期
14.2.5	8.27	安全系統架構及工程原則
14.2.7	8.30	委外開發
14.3.1	8.33	測試資訊
12.7.1	8.34	於稽核測試期間對資訊系統的保護

課程大綱

- ISMS標準發展與修訂背景
- 新舊版標準關鍵差異分析
- 新版標準條文理解與運用
- 新版標準 附錄A 安全控制措施之詮釋與運用

附錄 A（規範性）資訊安全控制措施參考

- 表 A.1 所列之各項資訊安全控制措施，乃直接取自 ISO 27002 [1] 之第 5 節至第 8 節，並與之調和，且於內文中與 6.1.3 一起使用。
- 控制措施條文中未有強制性選項 (即適用或不適用)
- 增加五大控制措施屬性可供選擇、創造資安廣度和深度，亦可自建適用之屬性以滿足本身需求。
- 不強調「控制目標」，而以「**目的**」來取代。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.1	資訊安全政策	**控制** 資訊安全政策和特定主題之**政策應被定義**、獲管理層核准、發布、傳達給相關人員及相關的利害關係者並取得其認可，並於計劃的時間間隔及發生重大變化時進行審查。
A.5.2	資訊安全的角色與職責	**控制** 應根據組織的需要，定義和分配資訊安全角色與職責。
A.5.3	職務區隔	**控制** 相互衝突的職務和責任領域應被區隔。
A.5.4	管理階層責任	**控制** 管理階層應要求所有人員按照組織已制定的資訊安全政策、特定主題之政策及程序運行資訊安全。
A.5.5	與權責機關的聯繫	**控制** 組織應與有關之權責機關建立並保持聯繫。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.6	與特殊利害關係者的聯繫	**控制** 組織應與特殊利害關係者或其他專家安全論壇和專業協會建立及保持聯繫。
A.5.7	**威脅情資**	**控制 (新增)** 應蒐集和分析與資訊安全威脅有關的資訊以產出威脅情資。

簡短討論1：如何偵蒐與運用「威脅情資」

- 可依貴組織之實務需求討論適切的實務作法，將有助控制措施有效施行。（以下之此討論並無標準解答）

威脅情資 - 實作指引

控制措施	目的	指引	實務做法
應蒐集和分析與資訊安全威脅有關的資訊以產出威脅情資。	提供對組織之威脅環境的認知，以便組織得以採取適當的緩解行動。	蒐集並分析有關現存或新興威脅的資訊，以使： a) 促進具見識的知情行動，以防止威脅對組織造成傷害； b) 減少此類威脅的衝擊。	1. 訂定威脅情資作業程序 2. 選擇來源，例如：TWCERT、CVE等 3. 管控協威脅情資之蒐集、分析、處理、運用、溝通及分享。 4. 建議修訂資安事件程序書

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.8	專案管理的資訊安全	**控制** 資訊安全應整入專案管理之中。
A.5.9	資訊和其它相關資產的清冊	**控制** 應發展並維持資訊和其它相關資產（包括擁有者）的清冊。
A.5.10	資訊和其它相關資產之可被接受的使用	**控制** 對資訊處理及其他相關資產，其可被接受的使用規則及程序，應予識別、文件化及實施。
A.5.11	資產歸還	**控制** 人員和其他適當的利害關係者應在其聘僱、合約或協議變更或終止時歸還其擁有的所有組織資產。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.12	資訊分類	**控制** 資訊應根據組織基於機密性、完整性、可用性及相關利害關係者要求的資訊安全需要進行分類。
A.5.13	資訊標示	**控制** 應根據組織採用的資訊分類方案，發展和實施一套適當的資訊標示程序。
A.5.14	資訊傳輸	**控制** 組織內部以及組織與其他各方之間的資訊傳輸規則、程序或協議，應適用於所有類型的傳輸設施。
A.5.15	存取控制	**控制** 應基於營運和資訊安全要求，建立和實施對資訊和其它相關資產之實體面和邏輯面的存取控制規則。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.16	身份管理	**控制** 應管理身份資訊的完整生命週期。
A.5.17	驗證資訊	**控制** 鑑別（身份）資訊的分配和管理應由一個管理過程來管控，包括告知人員關於鑑別資訊的適切處理。
A.5.18	存取權限	**控制** 應根據組織的特定主題政策和存取控制規則，來提供、審查、修改和移除對資訊和其它相關資產的存取權限。
A.5.19	供應商關係的資訊安全	**控制** 應識別及實施過程和程序，以針對使用供應商產品或服務相關的資訊安全風險進行管理。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.20	供應商協議內的資訊安全要求	**控制** 應依據供應商關係的類別，建立及議定相關的資訊安全要求。
A.5.21	管理資通技術（ICT）供應鏈的資訊安全	**控制** 應定義並實施過程和程序，以管理與 ICT 產品和服務供應鏈相關的資訊安全風險。
A.5.22	**供應商服務之監控、審查及變更管理**	**控制** 組織應定期監控、審查、評估並管理供應商資訊安全實務和服務交付的變更。
A.5.23	**使用雲端服務之資訊安全**	**控制(新增)** 應根據組織的資訊安全要求建立獲取、使用、管理和退出雲端服務的流程。

簡短討論2：如何確保雲端服務之資訊安全

- 識別使用雲端服務可能之資訊安全風險
- 使用雲端服務之資訊安全-實作指引

控制措施	目的	指引	實務做法
應根據組織的資訊安全要求建立獲取、使用、管理和退出雲端服務的流程。	為雲端服務的使用明訂和管理資訊安全。	組織應建立並就使用雲端服務的特定主題政策與所有利害關係者進行溝通。 組織應定義並傳達其打算如何管理與雲端服務之使用所相關的資訊安全風險。	1. 訂定雲端服務作業程序（委外作業程序） 2. 選擇服務、訂定協議、管控安全、定期查核、服務水準、日誌紀錄、變更管理、安全退出。 3. 風險分析、營運持續 4. 建議修訂委外作業程序書

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.24	資訊安全事故管理規劃與準備	**控制** 組織應透過定義、建立並溝通資訊安全事故管理過程、角色和職責，以規劃並準備對資訊安全事故的管理。
A.5.25	資訊安全事件的評定與決策	**控制** 組織應評定資訊安全事件並決定是否將其歸類為資訊安全事故。
A.5.26	對資訊安全事故的回應	**控制** 應依照文件化程序回應資訊安全事故。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.27	從資訊安全事故中學習	**控制** 從資訊安全事故中獲得的知識予以應用，以強化與改善資訊安全控制措施。
A.5.28	證據的蒐集	**控制** 組織應建立並實施與資訊安全事件相關之證據的識別、蒐集、獲取及保存程序。
A.5.29	**中斷期間的資訊安全**	**控制** 組織應規劃如何於中斷期間將資訊安全維持在適當的水準。
A.5.30	為營運持續性做好資通技術（ICT）的準備	**控制(新增)** 應基於營運持續性目標和 ICT 持續性要求來規劃、實施、維護並測試 ICT 準備情形。

簡短討論3：如何為營運持續性做好ICT的準備

- 先識別BIA、RPO、RTO
- 使用ICT 備妥供用於營運持續 - 實作指引

控制措施	目的	指引	實務做法
應基於營運持續性目標和ICT 持續性要求來規劃、實施、維護並測試 ICT 準備情形。	確保當發生中斷時，組織資訊和其它相關資產的可用性。	組織應確保以下： a) 有適當的組織架構，以準備、減輕和因應由具有必要責任、權力與能力的人員來支援發生的中斷； b) ICT 持續性計劃，包括詳細說明組織計劃如何管理 ICT 服務中斷的因應和恢復程序 c) ICT 持續性計劃。	1. 訂定ICT持續性計劃（以業務流程分析資訊系統）。 2. 設定營運持續編組。 3. 執行演練驗證計劃是否可行。 4. 建議修訂營運持續管理程序書。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.31	法律、法令、法規及契約要求	**控制** 資訊安全相關的法律、法令、法規及契約要求事項，以及組織滿足這些要求的作法，應被識別、文件化並保持更新。
A.5.32	智慧財產權	**控制** 組織應實施適當的程序，以保護智慧財產權。
A.5.33	紀錄之保護	**控制** 應保護紀錄免遭遺失、破壞、偽造、未經授權的存取和未經授權的發布。
A.5.34	隱私與個人可識別資訊（PII）的保護	**控制** 組織應根據適用的法令、法規及合約要求，識別並符合有關維護隱私與保護 PII 的要求。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

A.5 組織控制措施		
A.5.35	資訊安全之獨立審查	**控制** 組織管理資訊安全的方法及其實施（包括人員、過程與技術），應按規劃的間隔時間或發生重大變更時進行獨立審查。
A.5.36	**資訊安全政策、規則與標準之遵循性**	**控制** 應定期審查對組織資訊安全政策、特定主題之政策、規則與標準的遵循情形。
A.5.37	文件化的作業程序	**控制** 資訊處理設施的作業程序應文件化，並讓需要的人員可取用。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

6	人員控制措施	
A.6.1	篩選	**控制** 應考量適用的法令法規、道德規範，及適度的營運要求、要存取的資訊分類和感知到的風險，對所有將成為員工的候選者於加入組織之前及持續執行的基礎上進行背景核查。
A.6.2	聘僱條款與條件	**控制** 聘僱合約協議應敘明人員和組織對資訊安全的責任。
A.6.3	資訊安全認知、教育與培訓	**控制** 組織人員和相關的利害關係者應接受與其工作職能相關的適當資訊安全認知、教育與培訓，並定期更新其組織資訊安全政策、特定主題之政策及程序。
A.6.4	懲處程序	**控制** 應正式制定並傳達懲處程序，以對違反資訊安全政策的人員和其他相關的利害關係者採取行動。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

6	人員控制措施	
A.6.5	聘僱終止或變更後之責任	**控制** 應定義、執行並與相關人員和其他利害關係者溝通在聘僱終止或變更後仍然有效的資訊安全責任和義務。
A.6.6	機密性或保密協議	**控制** 反映組織對資訊保護所需的機密性或保密之協議，應由人員和其他相關的利害關係者所識別、文件化、定期審查及簽署。
A.6.7	遠距工作	**控制** 當人員遠距工作時，應實施安全措施，以保護在組織場域外存取、處理或儲存的資訊。
A.6.8	**資訊安全事件通報**	**控制** 組織應提供一種機制，供人員可透過適當管道及時通報觀察到或可疑的資訊安全事件。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

7	實體控制措施	
A.7.1	實體安全邊界	**控制** 應定義及使用安全周界，以保護包含資訊及其他相關聯資產之區域。
A.7.2	實體進出管制	**控制** 保全區域應藉由適切之入口控制措施及進出點加以保護。
A.7.3	辦公室、空間與設施的保護	**控制** 應設計並實施辦公室、空間與設施的實體安全。
A.7.4	實體安全監視	**控制(新增)** 應持續監視場域，以避免未經授權的實體進出。

簡短討論4：如何強化實體安全監控

- **實體安全監視 - 實作指引**

控制措施	目的	指引	實務做法
應持續監控場域以避免未經授權的實體存取。	偵測和阻止未經授權的實體存取。	應持續監控對容納關鍵系統之建築物： a) 安裝影像監控系統，例如閉路電視，以查看並記錄對組織場域內外敏感區域的存取。 b) 根據相關適用標準安裝並定期測試接觸、聲音或移動偵測器以觸發入侵者警報。 c) 使用這些警報覆蓋所有對外出入口和可存取的窗戶。無人區應隨時保持可告警狀態。	1. 安裝門禁、監控及警報(保全)系統。 2. 執行進出管制、定期查核、告警事件處理、記錄保存。 3. 系統應定期測試監控安全 4. 建議修訂實體環境程序書。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

7	實體控制措施	
A.7.5	對抗實體與環境威脅的保護	**控制** 應設計並實施對抗實體與環境威脅的保護，例如自然災害和其它對基礎設施蓄意或非蓄意的實體威脅。
A.7.6	在安全區域內工作	**控制** 應設計並實施在保全區域內工作的安全措施。
A.7.7	桌面淨空與螢幕淨空	**控制** 紙本和可移除（動）式儲存媒體的桌面淨空規則及資訊處理設施的螢幕淨空規則應被定義和適當執行。
A.7.8	設備安置與保護	**控制** 設備應被安全安置並受到保護。
A.7.9	場所外資產的安全	**控制** 場所外之資產應受到保護。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

7	實體控制措施	
A.7.10	儲存媒體	**控制** 儲存媒體應按照組織的分類方案與處理要求，於其獲取、使用、運送和處置的整體生命週期中受到管理。
A.7.11	支援之公用設施	**控制** 應保護資訊處理設施免受因支援之公用設施故障而導致的電力失效和其它中斷。
A.7.12	佈纜之安全	**控制** 應保護傳輸電力、資料或支援資訊服務的佈纜免受攔截、干擾或破壞。
A.7.13	設備維護	**控制** 應正確維護設備，以確保資訊之可用性、完整性與機密性。
A.7.14	設備的汰除或再使用之安全	**控制** 應核查包含儲存媒體的設備項目，以確保於汰除或再使用之前已移除或安全覆蓋任何敏感資料和授權軟體。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.1	使用者終端裝置	**控制** 應保護透過使用者終端裝置儲存、處理或可存取的資訊。
A.8.2	特權存取權限	**控制** 應限制並管理特權存取權限的分配和使用。
A.8.3	資訊存取限制	**控制** 應根據已建立的特定主題之存取控制政策限制對資訊和其它相關資產的存取。
A.8.4	程式源碼的存取	**控制** 應適當管理對程式源碼、開發工具和軟體庫的讀寫存取。
A.8.5	安全驗證	**控制** 應根據資訊存取限制和特定主題的存取控制政策，實施安全驗證技術與程序。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.6	容量管理	**控制** 資源的使用應被監控和調整，以符合當前和預期的容量要求。
A.8.7	防範惡意程式	**控制** 應透過適當的使用者認知，實施並支持防範惡意程式的保護。
A.8.8	技術漏洞的管理	**控制** 應取得關於使用中之資訊系統的技術脆弱性資訊，並且應評估組織對此類漏洞的暴露程度並應採取適當的措施。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.9	組態管理	**控制(新增)** 應建立、文件化、實施、監控和審查硬體、軟體、服務和網路的組態，包括安全組態。

簡短討論5：識別「組態管理」之要素

- 舉例資訊管理系統中，哪些資訊要素可列入組態管理。

組態管理 - 實作指引

控制措施	目的	指引	實務做法
應建立、文件化、實施、監控和審 查硬體、軟體、服務和網路的組 態，包括安全組態。	確保硬體、軟體、服務和網路在所 需的安全設定下 正常運行，並且 組態不會因未經授權或不正確的 變更而遭到異動。	組織應定義和實施流程和工具， 以為硬體、軟體、服務（例如雲端服務）和網路、 新安裝的系統以及運作中的系統 於其生命週期內執行定義好的組態（包括安全組態）。	1. 進行資產盤點時應清點其組態分類。 2. 建立各項組態基準並依基準執行組態管理 3. 確認各項基準現狀及變更。 4. 建議修訂資訊資產管理程序書，或新增組態管理程序書

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.10	資訊刪除	**控制(新增)** 當不再需要時，應刪除儲存於資訊系統、裝置或任何其它儲存媒體中的資訊。

簡短討論6：如何確認「資料刪除」之完整性

- 重點識別資訊的風險，刪除的時機與程序、結果的確認等。

資料刪除 - 實作指引

控制措施	目的	指引	實務做法
當不再需要時應刪除儲存於資訊系統、裝置或任何其它儲存媒體中的資訊。	防止不必要的敏 感資訊揭露並 遵守有關資訊刪 除的法令法規、 監管與合約要求。	當刪除系統、應用程式與服務上的資訊時，應考慮以下幾點： a)根據營運需求並考慮相關法令法規，以選擇刪除方法（如電子覆寫或加密抹除）； b)記錄刪除結果以作為證據； c)當採用服務供應商的資訊刪除服務時，向其獲取資訊刪除的證據。	1. 進行資產盤點時應清點**資訊保存週期**。 2. 建立各類型**資料刪除方式、週期及記錄格式**。 3. 執行**刪除並保存紀錄** 4. 建議**修訂資訊資產管理程序書**，或新增資訊管理程序書

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.11	資料遮蔽	**控制(新增)** 應根據組織關於**存取控制**與**其它相關的特定主題政策**以及營運要求使用資料遮蔽，並**將法律要求納入考量**。

簡短討論7：如何實現有效的「資料遮罩」

- 識別「資料遮罩」之稽核重點，例：加密、攪亂、置換及匿名化等資料遮罩技術，作業程序等。

資料遮罩 - 實作指引

控制措施	目的	指引	實務做法
應根據組織關於 存取控制與其它 相關的特定主題 政策以及營運要 求使用資料遮蔽，並將法律要求納入考量。	限制敏感資料（包括PII）的揭露，並遵守法令法規、監管和合約要求。	當需要考慮保護敏感資料（例如PII）時，組織應考量使用資料遮蔽、擬匿名化或匿名化等技術隱藏此類資料。 擬匿名化或匿名化技術可以隱藏PII，掩飾PII當事人或其它敏感資訊的真實身份、**斷開PII與PII當事人身份或其他敏感資訊之間的連結**。	1. 進行資產盤點時應確認資訊是否進行遮蔽。 2. 建立各類型資料遮蔽方式及記錄格式。 3. 執行遮蔽並保存紀錄。 4. 建議修訂資訊資產管理程序書，或新增資訊管理程序書。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.12	預防資料洩漏	**控制(新增)** 資料洩漏的預防措施應應用於處理、儲存或傳輸敏感資訊的系統、網路及任何其它裝置。

簡短討論8：如何預防「資料洩露」

- 重點識別資訊的風險 (重要性、威脅來源、弱點及洩露管道)、預防及管控程序等。

預防資料洩漏 - 實作指引

控制措施	目的	指引	實務做法
資料洩漏的預防措施應應用於處理、儲存或傳輸敏感資訊的系統、網路及任何其它裝置。	檢測並防止個人或系統未經授權地揭露和提取資訊。	組織應考慮以下事項以降低資料洩露的風險： a) 識別和分類資訊以防止洩露（例如個人資訊、訂價模式和產品設計）； b) 監控資料洩漏管道（例如電子郵件、檔案傳輸、行動設備和可攜式儲存裝置）； c) 採取措施防止資訊洩露（例如，隔離包含敏感資訊的電子郵件）。	1. 進行資產盤點時應識別及分類。 2. 整合各項資訊洩漏防護措施。 3. 利用控制措施屬性，管控資訊保護做法。 4. 建議**修訂資訊資產管理程序書**，或新增資訊管理程序書

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.13	資訊備份	**控制** 資訊、軟體和系統的備份副本應按照議定的特定主題備份政策進行維護和定期測試。
A.8.14	資訊處理設施的備援	**控制** 資訊處理設施的實施應具有足以滿足可用性要求的備援。
A.8.15	日誌存錄	**控制** 記錄活動、異常、錯誤和其他相關事件的日誌，應被產生、儲存、保護和分析。
A.8.16	**活動監測**	**控制(新增)** 應監測網路、系統和應用程式的異常行為，並採取適當行動以評估潛在的資訊安全事故。
A.8.17	時脈同步	**控制** 組織使用的資訊處理系統之時脈應與核准的時間源同步。

簡短討論9：如何落實「監視活動」的預防效果

- 重點識別資訊存取、網路活動之紀錄保留與監控，相關因應程序。

活動監控 - 實作指引

控制措施	目的	指引	實務做法
應監測網路、系統和應用程式的異常行為，並採取適當行動以評估潛在的資訊安全事故。	偵測異常行為和潛在的資訊安全事故。	監控範圍和級別應根據業務和資訊安全要求並結合相關法律法規確定。應使用通過監測工具進行的持續監測。應根據組織的需要和能力，即時或定期進行監控。應將異常事件傳達給相關方，以改進以下活動：稽核、安全評估、漏洞掃描和監控（見 5. 25）。 應制定程式以及時回應來自監控系統的積極指標，以儘量減少資安事件（見 5.26）對資訊安全的影響。	1. 檢討現有監控工具，若有不足宜購置相關工具。 2. 整合監控、漏洞及資安事件通報。 3. 針對監控紀錄執行分析、處理及運用。 4. 修訂資安事件程序書、作業安全程序書。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.18	特權的公用程式之使用	**控制** 應限制並嚴格管控能夠篡越系統和應用程式控制的公用程式之使用。
A.8.19	運作中系統上的軟體安裝	**控制** 應實施程序和措施以安全地管理運作中系統上的軟體安裝。
A.8.20	網路安全	**控制** 應保護、管理和管控網路及網路設備以保護系統和應用程式中的資訊。
A.8.21	網路服務的安全	**控制** 應識別、實施並監控網路服務的安全機制、服務水準及服務要求。
A.8.22	網路區隔	**控制** 資訊服務、使用者與資訊系統的群組應於組織的網路中區隔。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.23	網頁過濾	**控制 (新增)** 應管理對外部網站的存取，以減少接觸惡意的內容。

簡短討論10：如何實現有效的「網頁過濾」

- 重點識別SSL憑證、隱私權聲明、檢視網域及WEB所有權等。

網頁過濾 - 實作指引

控制措施	目的	指引	實務做法
應管理對外部網站的存取，以減少曝露於惡意的內容。	保護系統免受惡意軟體的危害並防止存取未經授權的網頁資源。	組織應降低員工存取包含非法資訊或已知包含病毒或網路釣魚材料的網站的風險。一種通過阻止相關網站的 IP 位址或域來實現此目的的技術。一些流覽器和反惡意軟體技術會自動執行此操作或可以配置為執行此操作組織應確定人員應該或不應該訪問的網站類型。 在部署此控制之前，組織應建立安全和適當使用線上資源的規則，包括對不受歡迎或不適當的網站和基於網站的應用程式的任何限制。	1. **檢討現有防火牆或網路控制工具**，依照指引執行相關設定。 2. **教育訓練教材中應放入本項控制措施**。 3. 定期檢討各項限制規則並更新規則。 4. 修訂網路安全程序書。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.24	密碼學的使用	**控制** 應定義並實施有效使用密碼學的規則，包括密碼學的金鑰管理。
A.8.25	安全之開發生命週期	**控制** 應建立並運用軟體和系統的安全開發規則。
A.8.26	應用程式安全要求	**控制** 於開發或獲取應用程式時，應識別、明訂並核准資訊安全要求。
A.8.27	安全系統架構與工程原則	**控制** 工程安全系統之原則，應予建立、以文件記錄、維持及應用於所有資訊系統開發活動。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.28	安全編碼	**控制(新增)** 軟體開發應採用安全編碼原則。

簡短討論11：瞭解安全的軟體工程原則

- 重點識別SSDLC相關稽核實務。

安全編碼 - 實作指引

控制措施	目的	指引	實務做法
軟體開發應採用安全編碼原則。	確保安全編寫軟體，從而減少軟體中潛在資訊安全漏洞的數量。	組織應建立組織範圍的流程，為安全編碼提供良好的管理。應建立和應用最低安全基準。此外，此類流程和管理應擴展到涵蓋來自協力廠商的軟體元件和開源軟體。 組織應監控現實世界的威脅以及有關軟體漏洞的最新建議和資訊，以通過持續改進和學習來指導組織的安全編碼原則。這有助於確保實施有效的安全編碼實踐，以應對快速變化的威脅形勢。	1. 檢討現有**軟體開發流程將安全要求導入開發過程中**。 2. 管控各項元件（含第三方）之安全性。 3. 執行必要的測試及安全性檢測工作。 4. 結合構型管理。 5. **修訂資訊系統開發維護程序書**。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.29	開發與驗收的安全測試	**控制** 應於開發生命週期中定義並實施安全測試流程。
A.8.30	委外開發	**控制措施** 組織應指導、監控並審查與委外系統開發相關的活動。
A.8.31	**區隔開發、測試與正式環境**	**控制** 應區隔並保護開發、測試與正式環境。
A.8.32	**變更管理**	**控制** 資訊處理設施和資訊系統的變更應依循變更管理程序。
A.8.33	測試資訊	**控制** 應適當地選擇、保護並管理測試資訊。

附錄 A（規範性）資訊安全控制措施參考

表 A.1 - 資訊安全控制

8	技術控制措施	
A.8.34	於稽核測試期間對資訊系統的保護	**控制** 稽核測試與其它涉及評鑑運作中系統的保證活動，應於測試人員和適當的管理人員之間進行規劃並同意。

資訊安全控制措施-五大屬性

控制措施種類	資訊安全特性	網路安全概念	運作能力	安全領域
#預防性	#機密性 #完整性 #可用性	#防護	#系統與網路安全 #資訊保護	#治理與生態系統 #保護


THANK YOU