資訊安全管理制度國際標準(ISO 27001:2022)簡介

八月 2023

pwc 資誠

黃承漢 經理

聯絡資訊:
Office: +886 2 2729 6666 ext. 23227
Mobile: +886 978131732
Email: michael.a.huang@pwc.com

| 經歷 |

- 資誠聯合會計師事務所 風險及控制服務 經理
- 資誠聯合會計師事務所 風險及控制服務 資深顧問
- 資誠企業管理顧問股份有限公司　資深顧問
- 華碩電腦 IT運營專案課 資安工程師
- 曜揚科技 技術服務部組長
- 曜揚科技 技術服務部 系統工程師

| 專長 |

- 資訊安全管理制度(ISMS)輔導諮詢服務
- 個人資訊管理系統(PIMS)輔導諮詢服務
- 品質管理(QMS)輔導諮詢服務
- 營運持續管理系統(BCMS) 輔導諮詢服務
- 資訊科技服務管理(ITSM)輔導諮詢服務
- 資訊安全評估
- PCIDSS
- 資安治理成熟度分析
- 資通安全管理法應辦事項因應
- 資訊風險管理
- 防毒軟體、DLP解決方案導入

| 專業資格和證照 |

- PMP(Project Management Professional)國際專案管理師認證2012~2023年
- EC-Council CHFI v8資安鑑識調查專家認證
- ISO 27001:2005、2013、2022資訊安全管理制度Lead Auditor
- BS 10012:2017 個人資訊管理制度 Lead Auditor
- ISO 29100:2011 個人隱私保護管理隱私框架Lead Auditor
- ISO 27018:2014雲端個人隱私資料保護管理制度Lead Auditor
- ISO 27701:2019 個人資料隱私管理系統 Lead Auditor
- ISO 22301:2019 營運持續管理制度Lead Auditor
- SGS「資通系統防護基準–合規技術專員」證書
- ITIL v3 Foundation 認證
- Trend Certified Security Expert 趨勢認證資訊安全專家認證
- 微軟MCTS(Hyper-V 虛擬化解決方案)
- 微軟MCTS(Exchange 2010)
- 微軟MCTS(SharePoint 2010, Configuring)
- 中華數位SPAM SQR專業證照

Agenda

1. 關於資訊安全管理系統(ISO 27001:2022)
2. 新版ISO27001主條文新增要求與控制措施簡介
3. 新版ISO27001控制措施轉版秘訣大公開
4. 新版ISO27001控制措施要求綜合說明(打通任督二脈)

1

關於資訊安全管理系統 (ISO 27001:2022)

27001名稱異動

ISO/IEC 27001:2013

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

資訊科技— 安全技術 —資訊安全管理系統 要求

標準名稱修改

ISO/IEC 27001:2022

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

資訊安全、網宇安全和隱私保護——資訊安全管理系統 要求

控制類別

控制類別數量由14類整併為4大類

- A.5 資訊安全政策
- A.6 資訊安全組織
- A.7 人力資源安全
- A.8 資產管理
- A.9 存取控制
- A.10 密碼技術
- A.11 實體與環境安全
- A.12 作業安全
- A.13 通訊安全
- A.14 系統之取得、開發與維護
- A.15 供應商管理
- A.16 資訊安全事故管理
- A.17 營運持續管理之資訊安全面向
- A.18 遵循性

ISO 27001:2013

ISO/IEC FDIS 27001:2022

- 37 Controls — **A5. 組織控制**
- 8 Controls — **A6. 人員控制**
- 14 Controls — **A7. 實體控制**
- 34 Controls — **A8. 技術控制**

控制項目數量

由原先114個控制項目調整為93個控制項目

New Contols說明
詳見下一章節介紹

由原先一個或多個控制項目
整合成一個控制項目
將列於後附投影片

ISO/IEC
27001:2013

將列於後附投影片

ISO/IEC
27001:2022

控制措施數量(整合合併24項)

2022	2013	項目名稱
5.1	05.1.1、05.1.2	資訊安全政策
5.8	06.1.5、14.1.1	專案管理中的資訊安全
5.9	08.1.1、08.1.2	資訊和其它相關資產的清查盤點
5.10	08.1.3、08.2.3	資訊和其他相關資產的可接受使用
5.14	13.2.1、13.2.2、	資訊傳遞
5.15	09.1.1、09.1.2	存取控制
5.17	09.2.4、09.3.1、	認證資訊
5.18	09.2.2、09.2.5、	存取權限
5.22	15.2.1、15.2.2	供應商服務之監控、審查及變更管理
5.29	17.1.1、17.1.2、17.1.3	中斷期間的資訊安全
5.31	18.1.1、18.1.5	識別法令法規、監管與合約要求
5.36	18.2.2、18.2.3	資訊安全政策、規則與標準之遵循性
6.8	16.1.2、16.1.3	資訊安全事件通報
7.2	11.1.2、11.1.6	實體進出管制
7.10	08.3.1、08.3.2	儲存媒體
8.1	06.2.1、11.2.8	使用者端點設備
8.8	12.6.1、18.2.3	技術漏洞的管理
8.15	12.4.1、12.4.2	日誌存錄
8.19	12.5.1、12.6.2	在作業系統上安裝軟體
8.24	10.1.1、10.1.2	密碼學的使用
8.26	14.1.2、14.1.3	應用程式安全要求
8.29	14.2.8、14.2.9	開發與驗收的安全測試
8.31	12.1.4、14.2.6	區隔開發、測試與正式環境
8.32	12.1.2、14.2.2	變更管理

控制措施數量(改變名稱22項)

2022	2013	項目名稱
5.19	15.1.1	供應商關係中的資訊安全
5.20	15.1.2	供應商協議內的資訊安全要求
5.21	15.1.3	管理 ICT 供應鏈中的資訊安全
5.24	16.1.1	資訊安全事件管理規劃和準備
5.25	16.1.4	資訊安全事件的評定與決策
5.34	18.1.4	PII 的隱私和保護
6.5	07.3.1	終止或改變工作後的責任
6.7	06.2.2	遠端工作
7.1	11.1.1	實體安全邊界
7.7	11.2.9	桌面淨空與螢幕淨空
7.9	11.2.6	場外資產的安全

2022	2013	項目名稱
8.2	9.2.3	特權存取權限
8.4	9.4.5	程式源碼的存取
8.5	09.4.2	安全認證
8.7	12.2.1	防範惡意軟體
8.14	17.2.1	資訊處理設施的備援
8.20	13.1.1	網路安全
8.22	13.1.3	網路區隔
8.25	14.2.1	安全的開發生命週期
8.27	14.2.5	安全系統架構和工程原理
8.33	14.3.1	測試資訊
8.34	12.7.1	在稽核測試期間保護資訊系統

2

新版ISO27001主條文新增要求與控制措施簡介

主條文新增要求

本文異動說明

- 整體架構未有改變
- 主要針對主條文多做說明，要求定義實施ISMS所需的流程及之間的相互作用或明確要求組織內溝通與資訊安全有關的角色。

本文	異動內容
4 組織全景	**異動三條內容**
5 領導作為	**異動二條內容**
6 規劃	**異動三條內容**
7 支援	**異動一條內容**
8 運作	**異動一條內容**
9 績效評估	**異動一條內容**
10 改善	**異動一條內容**

4.1 瞭解組織及其全景

異動備考之內容

組織應決定與其目的有關且影響達成其資訊安全管理系統預期成果能力之外部及內部議題。
備考：決定此等議題，係指建立於CNS 31000之 5.4.1 中所考量的組織外部及內部全景。

說明：

因應ISO 31000已更新為2018版而調整，對現行作業無顯著影響。

4.2 瞭解關注方之需要及期望

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。
備考：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 瞭解關注方之需要及期望
組織應決定下列事項 ：
(a) 與資訊安全管理系統有關之關注各方。
(b) 此等關注方之相關要求事項。
(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(ISMS)因應。
備考：關注方之要求事項可能包括法律及法規要求事項，以及契約義務。

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 組織 依本標準之要求事項，建立、實作、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。

5.1 領導及承諾

異動備考之內容

備考：本標準所提及之〝營運〞，能廣義詮釋為對組織存在目的具核心意義之該等活動。

說明：

強調「營運(Business)」可擴大解釋為組織之核心活動(附錄A將持續出現此字眼)

5.3 組織角色、責任及權限

異動備考之內容

備考：最高管理階層亦可指派報告組織內資訊安全管理系統績效之責任及權限。

說明：

強調於組織內進行職責與授權溝通。

6.1 因應風險及機會之行動

異動備考之內容

變更針6.1.3 附錄A之用詞：

備考 2. 附錄 A 包含可能之資訊安全控制措施清單。本標準之使用者參照附錄 A，以確保未忽略必要的資訊安全控制措施。

說明：

從全面的資安控制清單(a list of comprehensive information security controls)改成可能的資安控制清單(a list of possible information security controls)，僅為用詞上的改變，對現行輔導實務作業應無影響。

6.2 資訊安全目標及其達成之規劃

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；
d)經過溝通 且
e)適當時作更新 。

ISO 27001:2022

6.2 資訊安全目標及其達成之規劃
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) 可量測(若可行)。
(c) 考量適用之資訊安全要求事項，以及風險評鑑及風險處理的結果。
(d) 受監視。
(e) 被傳達。
(f) 於適切時，更新之。
(g) 以文件化資訊提供。

6.3 變更之規劃

新增之內容

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。

說明：

1. 新增條款「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」於以往的ISMS條文中並未強調PDCA循環中，從Action（例如：矯正措施）回到Planning（例如：內外部議題識別、利害相關團體要求識別、風險情境識別、風險處理方式、適用性聲明、資安目標等）的流程，新增之6.3即為填補該空缺。
2. 現行作業可能並未強調該流程，故為了因應此條款，建議將此條款寫入資安政策中。實作上則可以於管理審查會議簡報等文件中提及變更之規劃事項，以展現對此條款之符合性。

7.4 溝通或傳達

ISO 27001:2013

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

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) 溝通或傳達事項。
(b) 溝通或傳達時間。
(c) 溝通或傳達對象。
(d) 溝通或傳達方式。

8.1 運作之規劃及控制

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 運作之規劃及控制
組織應規劃、 實作及控制符合要求事項所需之過程，並藉由下列方式，實作第 6 節中所決定的行動：
— 建立過程之準則 。
— 依準則實作過程之控制措施。
應保存應提供文件化資訊 ，其程度須具足以達成其過程已依規劃執行之信心。
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負面效果。
組織應確保與資訊安全管理系統相關外部所提供之過程、產品或服務受控制。

9.1 監督、量測、分析及評估

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

組織應決定下列事項 ：
(a) 需要監督及量測之事項，包括資訊安全過程及控制措施 。
(b) 監督、量測、分析及評估之適用方法，以確保有效的結果。所選擇之方法宜產生適於比較及可重製視為有效的結果。
(c) 應執行監督及量測之時間。
(d) 應執行監督及量測之人員。
(e) 監督及量測結果應分析及評估之時間。
(f) 應執行分析及評估此等結果之人員。
應具備文件化資訊，作為結果之證據。
組織應評估資訊安全績效及資訊安全管理系統之有效性。

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
9.3
管理審查
9.3.2 管理審查輸入
新增輸入事項：
c)與資訊安全管理系統相關關注方之需要及期望的變更。

要求架構變更(10.改善)

ISO 27001:2013

10.1
不符合事項與矯正措施
10.2
持續改善

ISO 27001:2022

10.1
持續改善
10.2
不符合事項及矯正措施

控制措施簡介

§5 組織控制措施

5.1 資訊安全政策：

資訊安全政策及主題特定政策應予以定義，由管理階層核可、發布、傳達予相關人員及相關關注方，且其係知悉，並依規劃期間及發生重大變更時審查。

5.2 資訊安全之角色與責任：

應根據組織需要，定義並配置資訊安全之角色及責任。

5.3 職務區隔：

衝突之職務及衝突的責任範圍應予以區隔。

5.4 管理階層責任：

管理階層應要求所有人員工，依組織所建立資訊安全政策、主題特定政策及程序，實施資訊安全。

5.5 與權責機關之聯繫：

組織應建立並維持與相關權責機關之聯繫。

5.6 與特殊關注群組之聯繫：

組織應建立並維持與各特殊關注群組或其他各專家安全論壇及專業協會之聯繫。

§5 組織控制措施

5.7 威脅情資：

應蒐集並分析與資訊安全威脅相關之資訊，以產生威脅情資。

5.8 專案管理之資訊安全：

資訊安全應整合入專案管理中。

5.9 資訊及其他相關聯資產之清冊：

應製作並維護資訊及其他相關聯資產(包括擁有者)之清冊。

5.10 可接受使用資訊及其他相關聯資產：

應識別、書面記錄及實作對處置資訊及其他相關聯資產之可接受使用的規則及程序。

5.11 資產之歸還：

適切時，人員及其他關注方於其聘用、契約或協議變更或終止時，應歸還其持有之所有組織資產。

5.12 資訊之分類分級：

資訊應依組織之資訊安全需要，依機密性、完整性、可用性及相關關注方要求事項分類分級。

§5 組織控制措施

5.13 資訊之標示：

應依組織所採用之資訊分類分級方案，發展及實作一套適切的資訊標示程序。

5.14 資訊傳送：

應備妥資訊傳送規則、程序或協議，用於組織內及組織與其他各方間之所有形式的傳送設施。

5.15 存取控制：

應依營運及資訊安全要求事項，建立並實作對資訊及其他相關聯資產之實體及邏輯存取控制的規則。

5.16 身分管理：

應管理身份之整個生命週期。

5.17 鑑別資訊：

鑑別資訊之配置及管理應由管理過程控制，包括告知人員關於鑑別資訊的適切處理。

5.18 存取權限：

應依組織之存取控制的主題政策及規則，提供規定、審查、修改及刪除對資訊及其他相關聯資產之存取權限。

§5 組織控制措施

5.19 供應者關係中之資訊安全：

應定義並實作過程及程序，管理與供應者產品或服務之使用相關聯的資訊安全風險。

5.20 於供應者協議中闡明資訊安全：

應依供應者關係之形式，建立相關的資訊安全要求事項，並與各供應者議定。

5.21 管理ICT供應鏈中之資訊安全：

應定義並實作過程及程序，管理與ICT產品及服務供應鏈相關聯之資訊安全風險。

5.22 供應者服務之監視、審查及變更管理：

組織應定期監控、審查、評估及管理供應者資訊安全實務作法及服務交付之變更。

5.23 使用雲端服務之資訊安全：

應依組織之資訊安全要求事項，建立獲取、使用、管理及退出雲端服務的過程。

5.24 資訊安全事故管理規劃及準備：

組織應藉由定義、建立並溝通或傳達資訊安全事故管理過程、角色及責任，規劃並準備管理資訊安全事故。

§5 組織控制措施

5.25 資訊之評鑑及決策：

組織應評鑑資訊安全事件，並判定是否將其歸類為資訊安全事故。

5.26 對資訊安全事故之回應：

應依書面記錄程序，回應資訊安全事故。

5.27 由資訊安全事故中學習：

應使用由資訊安全事故中所獲得之知識，加強及改善資訊安全控制措施。

5.28 證據之收集：

組織應建立並實作程序，用以識別、蒐集、獲取及保存與資訊安全事件相關之證據。

5.29 中斷期間之資訊安全：

組織應規劃，如何於中斷期間維持資訊安全於適切等級。

5.30 營運持續之ICT備妥性：

應依營運持續目標及ICT資持續之要求事項，規劃、實作、維護及測試ICT備妥性。

§5 組織控制措施

5.31 法律、法令、法規及契約要求事項：

應識別、書面記錄及保持更新資訊安全相關法律、法令、法規、及契約之要求事項，以及組織為符合此等要求事項的作法。

5.32 智慧財產權：

該組織應實作適切程式，以保護智慧財產權。

5.33 紀錄之保護：

應保護記錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。

5.34 隱私及PII保護：

組織應依適用之法律、法規及契約的要求事項，識別並符合關於隱私保護及 PII保護之要求事項。

5.35 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的作法及其實作(包括員工、過程及技術)。

5.36 資訊安全政策、規則及標準之遵循性：

應定期審查組織資訊安全政策、主題特定政策、規則及標準之遵循性。

5.37 書面紀錄之運作程序：

應書面紀錄資訊處理設施之運作程序，並使所有需要的人員均可取得。

§6 人員控制措施

6.1 篩選：

對所有成為員工之候選者，應於其加入組織前，進行背景查證調查，且持續進行，同時將適用的法律、法規及倫理納入考量

，並宜相稱於營運要求事項，其將存取之資訊的分類分級及所察覺之風險。

6.2 聘用條款及條件：

聘用契約協議應敘明人員及組織對資訊安全之責任。

6.3 資訊安全認知及教育訓練：

組織及相關關注方之人員，均應接受與其工作職能相關的組織資訊安全政策、主題特定政策及程序之適切資訊安全認知及教育訓練，並定期更新。

6.4 獎懲過程：

應明確訂定並傳達獎懲過程，以對違反資訊安全政策之人員及其他相關關注方採取行動。

§6 人員控制措施

6.5 聘用終止或變更後之責任：

應對相關人員工及其他關注方定義、施行並傳達於聘用終止或變更後，仍保持有效之資訊安全責任及義務。

6.6 機密性或保密協議：

反映組織對資訊保護之需要的機密性或保密協議，應由人員及其他相關關注方，識別、書面紀錄、定期審查及簽署。

6.7 遠端工作：

應實作安全措施，當人員於遠端工作時，保護於組織場所外之存取、處理或儲存之資訊。

6.8 資訊安全事件通報：

組織應提供機制，供人員透過適切之管道，及時通報所觀察到或可疑的資訊安全事件。

§7 實體控制措施

7. 1 實體安全周界：

應定義及使用安全周界，以保護收容資訊和其他相關聯資產之區域。

7. 2 實體進入：

保全區域應藉由適切之進入控制措施及進出點加以保護。

7.3 保全辦公室、房間及設施：

應設計辦公室、房間及設施之實體安全並實作之。

7.4 實體安全監視：

應持續監視場所，防止未經授權之實體進出。

7.5 防範實體及環境威脅：

應設計並實作防範實體及環境威脅(諸如天然災害及其他對基礎設施之蓄意或非蓄意的實體威脅)之措施。

7.6 於安全區域內工作：

應制定和實施於安全區域內工作之安全措施。

7.7 桌面淨空及螢幕淨空：

應定義對紙本及可移除式儲存媒體之桌面淨空規則，以及對資訊處理設施的螢幕淨空規則，並適切實施之。

§7 實體控制措施

7. 8 設備安置及保護：

設備應安全安置並受保護。

7. 9 場所外資產之安全：

應保護場域外資產。

7.10 儲存媒體：

儲存媒體應依組織之分類分級方案及處理要求事項，於其獲取、使用、運送及汰除的整個生命週期內進行管理。

7.11 支援之公用服務事業：

應保護資訊處理設施免於電源失效，以及因支援之公用服務事業失效，所導致的其他中斷。

7.12 佈纜安全：

應保護傳送電源、資料或支援資訊服務之纜線，以防範竊聽、干擾或破壞。

7.13 設備維護：

應正確維護設備，以確保資訊之可用性、完整性及機密性。

7.14 設備汰除或重新使用之保全：

應查證包含儲存媒體之設備項目，以確保於汰除或重新使用前，所有敏感性資料及具使用授權的軟體已移除或安全覆寫。

§8 技術控制措施

8.1 使用者端點裝置：

應保護儲存於使用者端點裝置，由使用者端點裝置處理或經由使用者端點裝置可存取之資訊。

8.2 特殊存取權限：

應限制並管理特殊存取權限之配置及使用。

8.3 資訊存取限制：

應依已建立之關於存取控制的主題特定政策，限制對資訊及其他相關聯資產之存取。

8.4 對原始碼之存取：

應適切管理對原始碼、開發工具及軟體函式庫之讀寫存取。

8.5 安全鑑別：

安全鑑別技術及程序應依資訊存取限制及關於存取控制之主題特定政策實作。

8.6 容量管理：

資源之使用應受監視及調整，以符合目前容量要求及預期容量要求。

§8 技術控制措施

8.7 防範惡意軟體：

應實作防範惡意軟體之措施，並由適切的使用者認知支援之。

8.8 技術脆弱性管理：

應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，且應採取適切措施。

8.9 組態管理：

應建立、書面記錄、實作、監視並審查硬體、軟體、服務及網路之組態(包括安全組態)。

8.10 資訊刪除：

當於資訊系統、裝置或所有其他存儲媒體中之資訊不再屬必要時，應刪除之。

8.11 資料遮蔽：

應使用資料遮蔽，依據組織關於存取之主題特定政策及其他相關的主題特定政策，以及營運要求事項，並將適用法令納入考量。

8.12 資料洩露預防：

應將資料洩露預防措施，套用置處理、儲存或傳輸敏感性資訊之系統、網路及所有其他裝置。

§8 技術控制措施

8.13 資訊備份：

應依議定之關於備份的主題特定政策，維護資訊、軟體及系統之備份複本，並定期測試之。

8.14 資訊處理設施之多備：

資訊處理設施實作應充分多備(redundancy)，以符合可用性之要求事項。

8.15 存錄：

紀錄活動、異常、錯誤及其他相關事件之日誌，應產生、儲存、保護及分析之。

8.16 監視活動：

應監視網路、系統及應用之異常行為，並採取適切措施，以評估潛在資訊安全事故。

8.17 鐘訊同步：

組織所使用資訊處理系統之鐘訊，應與經認可的時間源同步。

8.18 具特殊權限公用程式之使用：

應限制並嚴密控制可能篡越系統及應用程式之控制措施的公用程式之使用。

§8 技術控制措施

8.19 運作中系統之軟體安裝：

應實作各項程序及措施，以安全管理對運作中系統安裝軟體。

8.20 網路安全：

應受保全、管理及控制網路與網路裝置，以保護系統及應用程式中之資訊。

8.21 網路服務之安全：

應識別、實作及監視網路服務之安全機制、服務等級及服務要求事項。

8.22 網路區隔：

應區隔組織網路中各群組之資訊服務、使用者及資訊系統。

8.23 網頁過濾：

應管理對外部網站之存取，以降低暴露於惡意內容。

8.24 密碼技術之使用：

應定義並實作有效使用密碼技術之規則(包括密碼金鑰管理)。

§8 技術控制措施

8.25 安全開發生命週期：

應建立並施行安全開發軟體及系統之規則。

8.26 應用系統安全要求事項：

開發或獲取應用系統時，應識別、規定並核可資訊安全要求事項。

8.27 安全系統架構及工程原則：

應建立、書面記錄及維護工程化安全系統之原則，並套用於所有資訊系統開發活動。

8.28 安全程式設計：

軟體開發應施行安全程式設計原則。

8.29 開發及驗收中之安全測試：

應於開發生命週期中定義並實作安全測試過程。

8.30 委外開發：

組織應指引、監視及審查與委外系統開發相關活動。

§8 技術控制措施

8.31 開發、測試與運作環境之區隔：

應區隔開發環境、測試環境與生產環境，並保全之。

8.32 變更管理：

資訊處理設施及資訊系統之變更，應遵循變更管理程序之。

8.33 測試資訊：

應適切選擇、保護及管理測試資訊。

8.34 稽核測試期間資訊系統之保護：

涉及運作中系統之評鑑的稽核測試及其他保證活動，應於測試者與適切管理階層間規劃並議定。

新增控制項

增加的控制項目- 5.7 威脅情資

控制措施	宜蒐集並分析與資訊安全威脅相關之資訊，以產生威脅情資。
目的	提供對組織威脅環境之認知 ，以便採取適切的減緩措施。
指引	蒐集並分析有關既有或新出現威脅之資訊，以便用於下列事項： (a) 促進採取知情行動，以防止威脅對組織造成傷害。 (b) 降低此等威脅之衝擊。
實務做法	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

增加的控制項目- 5.23 使用雲端服務之資訊安全

控制措施	宜依組織之資訊安全要求事項 ，建立獲取、使用、管理及退出雲端服務的過程。
目的	規定並管理使用雲端服務之資訊安全性。
指引	組織宜建立使用雲端服務之主題特定政策，並向所有相關關注方溝通或傳達。 組織宜定義並溝通或傳達其預期作法的延伸或一部分 (參照 5.21 及 5.22)。如何管理與使用雲端服務相關聯之資訊安全風險。其可能為組織如何管理外部各方所提供服務之既有
實務做法	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

增加的控制項目- 5. 30 營運持續之ICT備妥性

控制措施

宜依營運持續目標及 ICT 持續之要求事項，規 劃、實 作、維護及測試 ICT 備妥性。
((ICT , Information and Communication Technology)資訊與通訊科技

目的

確保於中斷期間，組織之資訊及其他相關聯資產的可用性。

指引

組織宜確保下列事項：
(a) 備妥適切之組織結構，以準備、減緩及回應中斷，此結構係由具必要責任、權限及專業能力的人員所支援
(b) ICT 持續計畫 (包含詳細敘明組織如何規劃管理 ICT 服務中斷之回應及復原程序)
(c) ICT 持續

實務做法

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

增加的控制項目- 7.4 實體安全監視

控制措施

宜持續監視場所，防止未經授權之實體進出。

目的

偵測並阻止未經授權之實體進出。

指引

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

實務做法

1.安裝門禁、監控及警報系統
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

增加的控制項目- 8.9 組態管理

控制措施	應建立、書面記錄、實作、監視並審查硬體、軟體、服務及網路之組態(包括安全組態)。
目的	確保硬體、軟體、服務及網路於所要求安全設定下正常運行，且組態未遭未經授權或不正確變更而更改。
指引	組織宜定義並實作過程及工具，以於硬體、軟體、服務（例:雲端服務）及網路、新安裝之系統，以及運作中系統的整個生命週期內，施行所定義之組態（包括安全組態）。
實務做法	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

增加的控制項目- 8.10 資訊刪除

控制措施

當於資訊系統、裝置或所有其他存儲媒體中之資訊不再屬必要時，應刪除之。

目的

防止敏感性資訊之非必要暴露，並遵循資訊刪除的法律、法令、法規及契約要求。

指引

刪除系統、應用程式及服務上之資訊時，宜考量下列事項：
(a)依營運要求，並考量相關法律及法規，選擇刪除方法（例:電子覆寫或密碼式抹除）。
(b)將刪除之結果記錄下來，作為證據。
(c)使用資訊刪除之服務供應者時，向其取得資訊刪除的證據。

實務做法

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

增加的控制項目- 8.11 資料遮蔽

控制措施

應使用資料遮蔽，依據組織關於存取之主題特定政策及其他相關的主題特定政策，以及營運要求事項，並將適用法令納入考量。

目的

限制內含PII敏感性資料的暴露，並遵循法律、法令、法規及契約要求

指引

於考量敏感性資料（例:PII ）之保護的情況下，組織宜考量使用諸如資料遮蔽、假名化或匿名化等技術隱藏此種資料。假名化或匿名化技術可以隱藏 PII ，偽裝 PII 當事人之真實身份或其他敏感性資訊，切斷 PII 與 PII 當事人身份間的連結，或其他敏感性資訊之間的連結。

實務做法

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

增加的控制項目- 8.12 資料洩露預防

控制措施

應將資料洩露預防措施，套用置處理、儲存或傳輸敏感性資訊之系統、網路及所有其他裝置。

目的

偵測並防止個人或系統未經授權揭露及擷取資訊。

指引

組織宜考量下列事項以降低資料洩露之風險：
(a)識別資訊並將其分類分級，以防範洩露（例:個人資訊、定價模型及產品設計）。
(b)監視資料洩漏管道（例:電子郵件、檔案傳送、行動裝置及和可攜式儲存裝置）。
(c)採取措施以防止資訊洩露（例:隔離包含敏感性資訊之電子郵件）。

實務做法

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

增加的控制項目- 8.16 監視活動

控制措施

應監視網路、系統及應用之異常行為，並採取適切措施，以評估潛在資訊安全事故。

目的

偵測異常行為及潛在資訊安全事故。

指引

宜依營運及資訊安全要求事項，並考量相關法律及法規，判定監視範圍及等級。宜於所定義留存期限內，維持監視紀錄。
宜使用經由監視工具進行之持續監視。宜依組織之需要及能力，即時或定期進行監視。
宜將異常事件傳達予關注方，以改善下列活動：稽核、安全評估、脆弱性掃描及監視（參照 5.25 ）。 宜備妥程序，以及時方式，回應源自監視系統之正向指標，以極少化不利事件（參照 5.26）對資訊安全的影響。

實務做法

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。

增加的控制項目- 8.23 網頁過濾

控制措施

應管理對外部網站之存取，以降低暴露於惡意內容。

目的

保護系統免受惡意軟體之危害，並防止存取未經授權的網頁資源。

指引

組織宜降低其人員存取含有非法資訊或已知含有病毒或網路釣魚資材之網站的風險。達成此目的之技術，係封鎖所關注網站之 IP 位址或網域。某些瀏覽器及防惡意軟體技術，自動執行此項操作或可設定組態以執行此項操作。
組織宜識別員工宜或不宜存取之網站型式。
在部署此控制措施前，組織宜建立安全及適切使用線上資源之規則，包括對非所欲或不適切之網站及網頁式應用程式的所有限制。

實務做法

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。

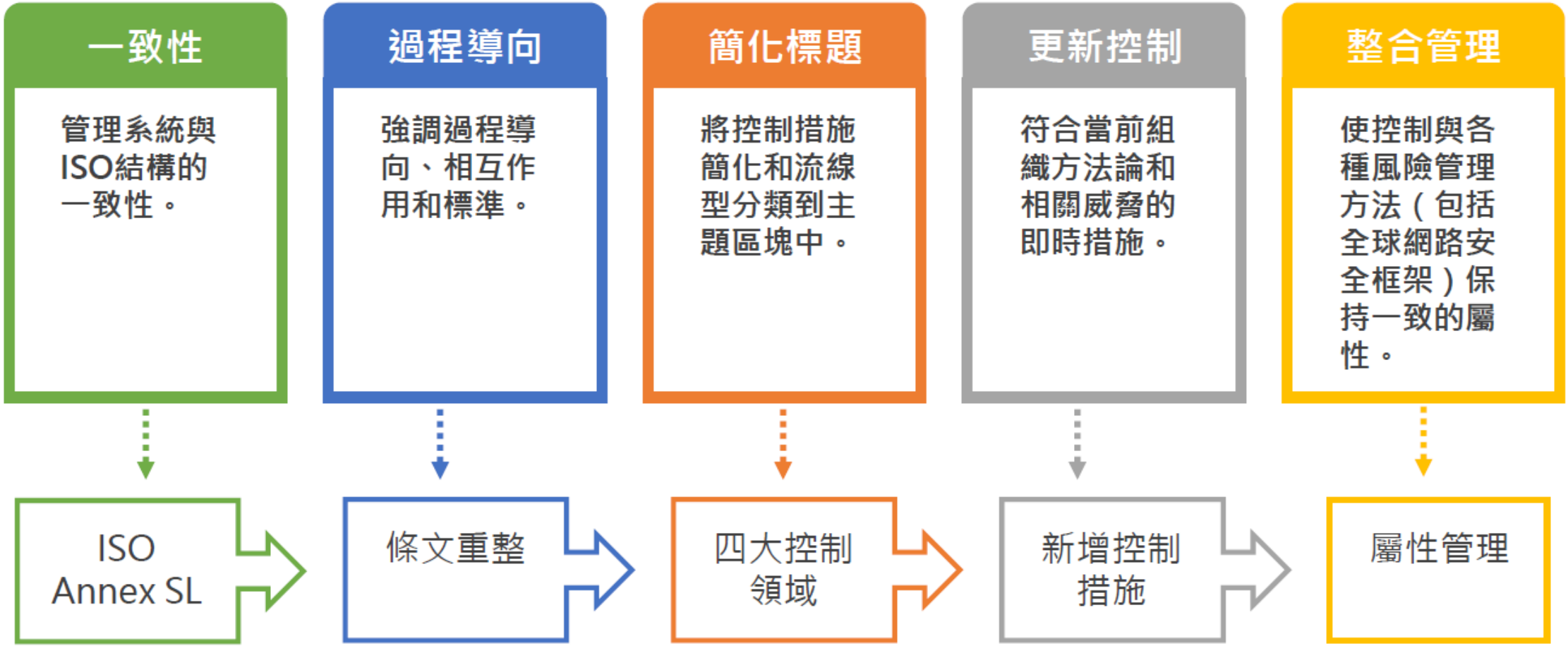
增加的控制項目- 8.28 安全程式設計

控制措施	軟體開發應施行安全程式設計原則。
目的	確保軟體係安全的撰寫，從而降低軟體中潛在資訊安全脆弱性之數量。
指引	組織宜建立全組織之過程，提供安全程式設計的良好治理。宜建立最低安全基準，並套用之。此外，此類過程及治理宜延伸至涵蓋源自第三方之軟體組件及開放原始碼軟體。 組織宜監視真實世界之威脅以關於軟體脆弱性的最新建議及資訊，以透過持續改善及學習，引導組織之安全程式設計原則。此可能有助於確保實作有效之安全程式設計實務作法， 以對抗快速變更的威脅形勢。
實務做法	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。

3

新版ISO27001控制措施轉版秘訣大公開

1.了解變化


一致性
管理系統與ISO結構的一致性。
過程導向
強調過程導向、相互作用和標準。
簡化標題
將控制措施簡化和流線型分類到主題區塊中。
更新控制
符合當前組織方法論和相關威脅的即時措施。
整合管理
使控制與各種風險管理方法（包括全球網路安全框架）保持一致的屬性。
ISO Annex SL
條文重整
四大控制領域
新增控制措施
屬性管理

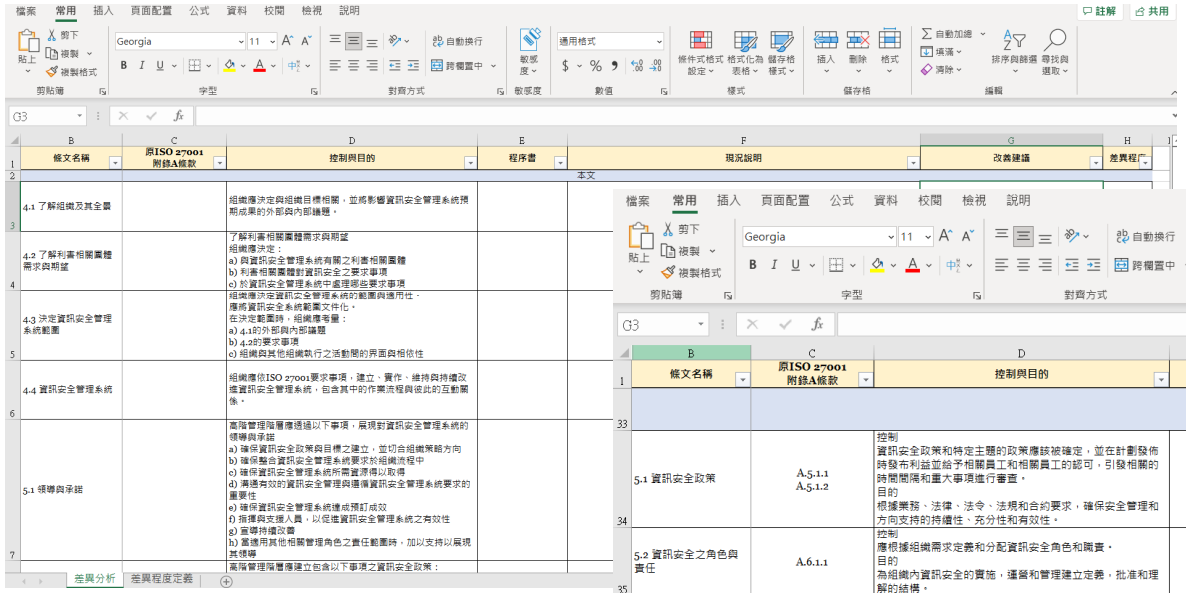
2.教育訓練

ISO 27001:2022基礎認知
控制措施實作變更說明

ISO 27001:2022
內部稽核

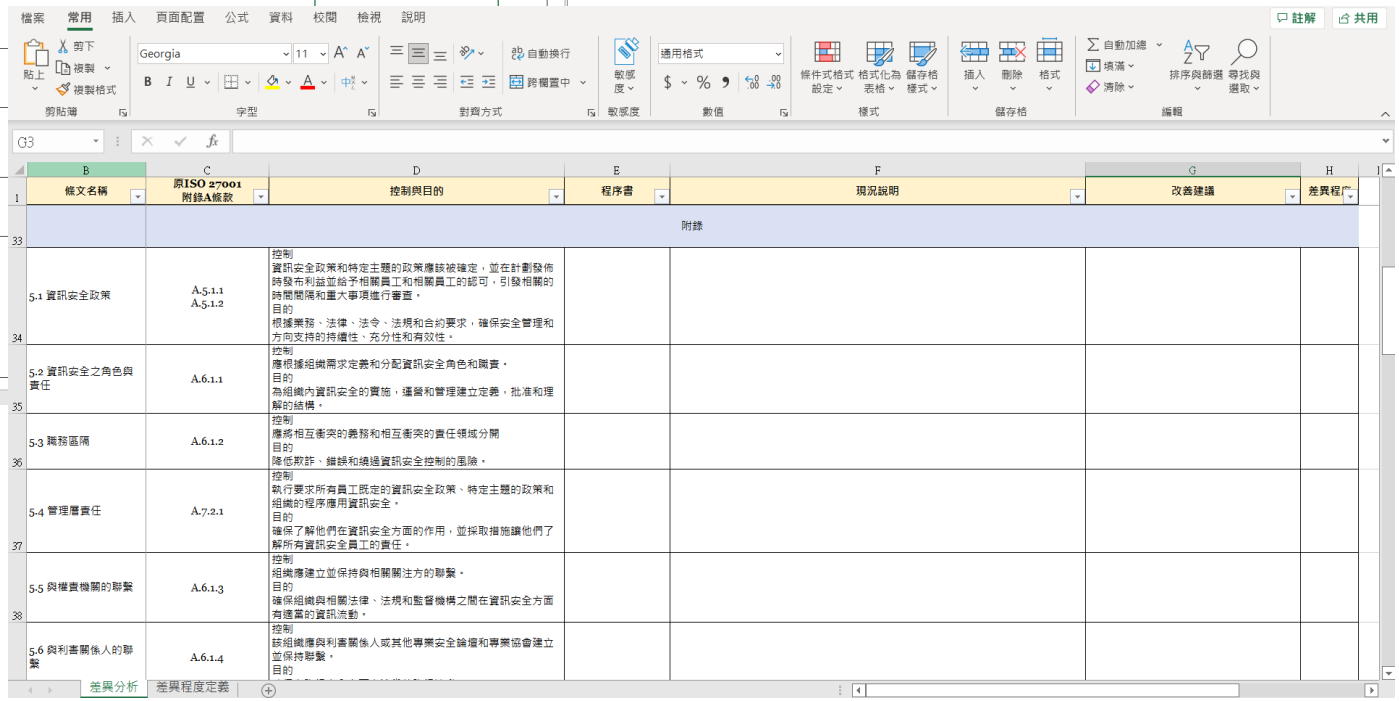
ISO 27001:2022
資訊資產盤點與風險評鑑

3.差異分析



條文名稱	原ISO 27001 附錄A條款	控制與目的	程序書	現況說明	改善建議	差異程
		本文				
4.1 了解組織及其全景		組織應決定與組織目標相關，並將影響資訊安全管理系統預期成果的外部與內部議題。				
4.2 了解利害相關團體需求與期望		了解利害相關團體需求與期望 組織應決定： a) 與資訊安全管理系統有關之利害相關團體 b) 利害相關團體對資訊安全之要求事項 c) 於資訊安全管理系統中處理哪些要求事項				
4.3 決定資訊安全管理系統範圍		組織應決定資訊安全管理系統的範圍與適用性，應將資訊安全系統範圍文件化。 在決定範圍時，組織應考量： a) 4.1的外部與內部議題 b) 4.2的要求事項 c) 組織與其他組織執行之活動間的界面與相依性				
4.4 資訊安全管理系統		組織應依ISO 27001要求事項，建立、實作、維持與持續改進資訊安全管理系統，包含其中的作業流程與彼此的互動關係。				
5.1 領導與承諾		高階管理階層應透過以下事項，展現對資訊安全管理系統的領導與承諾 a) 確保資訊安全政策與目標之建立，並切合組織策略方向 b) 確保整合資訊安全管理系統要求於組織流程中 c) 確保資訊安全管理系統所需資源得以取得 d) 溝通有效的資訊安全管理與遵循資訊安全管理系統要求的重要性 e) 確保資訊安全管理系統達成預訂成效 f) 指揮與支援人員，以促進資訊安全管理系統之有效性 g) 宣導持續改善 h) 支援用其他相關管理角色之責任範圍時，加以支持以展現其領導				
		高階管理階層應建立包含以下事項之資訊安全政策：				

差異分析 | 差異程度定義



條文名稱	原ISO 27001 附錄A條款	控制與目的	程序書	現況說明	改善建議	差異程
		附錄				
5.1 資訊安全政策	A.5.1.1 A.5.1.2	控制 資訊安全政策和特定主題的政策應該被確定，並在計劃發佈時發布利益並給予相關員工和相關員工的認可，引發相關的時間間隔和重大事項進行審查。 目的 根據業務、法律、法令、法規和合約要求，確保安全管理和方向支持的持續性、充分性和有效性。				
5.2 資訊安全之角色與責任	A.6.1.1	控制 應根據組織需求定義和分配資訊安全角色和職責。 目的 為組織內資訊安全的實施，運營和管理建立定義，批准和理解的結構。				
5.3 職務區隔	A.6.1.2	控制 應將相互衝突的義務和相互衝突的責任領域分開 目的 降低欺詐、錯誤和繞過資訊安全控制的風險。				
5.4 管理層責任	A.7.2.1	控制 執行要求所有員工既定的資訊安全政策、特定主題的政策和組織的程序應用資訊安全。 目的 確保了解他們在資訊安全方面的作用，並採取措施讓他們了解所有資訊安全員工的責任。				
5.5 與權責機關的聯繫	A.6.1.3	控制 組織應建立並保持與相關關注方的聯繫。 目的 確保組織與相關法律、法規和監督機構之間在資訊安全方面有適當的資訊流動。				
5.6 與利害關係人的聯繫	A.6.1.4	控制 該組織應與利害關係人或其他專業安全論壇和專業協會建立並保持聯繫。 目的				

差異分析 | 差異程度定義

4.風險分析

損害等級

等級	等級意義	損害價值	名譽損害	作業安全
1	Very Low（VL）	服務品質極輕度影響，未造成延期，財產極輕度損失，未發生違法情事。	無	無傷害或疾病。
2	Low（L）	服務品質輕度下降，造成輕微延期，財產輕度損失，未發生違法情事。	輕微（私下和解或調解），商譽受損造成營收輕度損失。	輕傷害或疾病。
3	Moderate（M）	服務品質中度下降，造成中等程度延期，財產中度損失，造成可能違法情事。	中度（沒有訴訟但上媒體），商譽受損造成營收中度損失。	中度傷害或疾病。
4	High（H）	服務品質高度下降，造成業務部分停頓，財產高度損失，有違法情事。	嚴重（有訴訟、上媒體），商譽受損造成營收高度損失。	重度輕傷害或疾病，未造成永久失能。
5	Very High（VH）	服務品質嚴重下降，所有核心業務停頓，財產極高度損失，嚴重違法。	極端嚴重（有訴訟、敗訴、上媒體），商譽受損造成營收極高度損失。	造成死亡、永久失能或不可復原。

發生可能性

等級	可能性說明	發生頻率
1	極低	超過 15 年才可能發生
2	低	每 5~15 年至少發生 1 次
3	中	每 3~5 年至少發生 1 次
4	高	每 1~3 年至少發生 1 次
5	極高	每年至少發生 2 次（含）以上

風險等級

發生可能性 \ 損害等級	1	2	3	4	5
5	C(5)	B(6)	B(7)	A(8)	A(9)
4	D(4)	C(5)	B(6)	B(7)	A(8)
3	D(3)	D(4)	C(5)	B(6)	B(7)
2	E(2)	D(3)	D(4)	C(5)	B(6)
1	E(1)	E(2)	D(3)	D(4)	C(5)

5.風險處理

參、 風險評鑑結果分析

綜合本案於民國 109 年 10 月 15 日至 11 月 12 日間，執行風險評鑑作業之結果，分述如下。

一、 風險評鑑彙整表

風險值高於 6 以上之風險的風險類別與風險情境，如下。

編號	正、負面風險	風險類別（或來源）	風險情境	業務內容	風險值	風險所有者	備註
							2019 年未再發生
NTUCC-AC10-RISK-006	負面	Operation Management Risk	關鍵系統異常造成服務中斷(軟體失效)	電子			
NTUCC-AC10-RISK-007	負面	Operation Management Risk	關鍵系統異常造成服務中斷(硬體故障)	虛擬主			

肆、 風險處理結果

根據風險評鑑結果，高於可接受風險值項目，提出風險處理計畫，執行結果如下。

編號	單位	風險處理措施	預計處理時程	原風險值	改善措施成本	剩餘風險值	監控日期及結果	實際完成日期	執行結果
NTUCC-AC10-RISK-006	作業組	依現有控制方式繼續執行，接受現有風險值。	已完成	6(高)	同仁每月執行人工檢測之人力成本（手上所有業務-預估 1 工作日）	6（高）	109/11/10	已完成	依現有控制方式繼續執行。
NTUCC-AC10-RISK-007	作業組	1. 定期檢測虛擬機是否安裝 VMware Patch。 2. 逐步增加自動檢測機制。 3. 依現有控制方式繼續執行，接受現有風險值。	1. 定期檢測虛擬機是否安裝 VMware Patch。 2. 110/06/30：資源使用率自動警報機制，如 Email 通知或 PRTG 機制	7(高)	1. Veeam 備份軟體已於 106 採購完畢。然每年需支付軟體保固費用。 2. 人力成本（預估每月 1.5 個工作人天）	7(高)	109/11/11	1.已完成； 2. 預計 110/06/30 完成	1. VMware Patch 已完成。 2. 110/06/30 檢視是否完成自動警報機制。 3. 依現有控制方式繼續執行。

6.適用性聲明

條款編碼	ISO/IEC 27001：2022	適用狀況		適用性說明
		是	否	
5 組織控制措施				
5.1	資訊安全政策	V		建立本處同仁及合作夥伴之資訊安全之依循準則，與確保本處之資訊安全政策之適切性
5.2	資訊安全之角色與責任	V		表達本處管理階層對資訊安全重視及執行之決心，並確保安全管理工作推動與進行之有效性，由本處資通安全推動小組負責整體之協調
5.3	職務區隔	V		確保安全管理工作有效性，由本處設置資通安全會報，並由各編組負責各項資訊安全管理工作。
5.4	管理層責任	V		確保同仁遵守安全規範
5.5	與權責機關的聯繫	V		確保本處符合主管機關等之要求。

7.文件修訂

文件編號	文件名稱	文件機密等級	相關表單編號	相關表單名稱	相關表單機密等級	發行日期	版次
NTUCC-AC10-IS1-01	資訊安全政策	一般				104.06.16	1.0
NTUCC-AC10-IS2-01	資訊安全組織管理程序書	限閱				104.07.20	1.0
			NTUCC-AC10-IS4-001	資訊安全組織成員表	限閱	108.06.18	1.0
			NTUCC-AC10-IS4-002	外來文件一覽表	限閱	109.09.18	1.1
			NTUCC-AC10-IS4-003	外部單位聯絡清單	限閱	108.07.23	1.0
NTUCC-AC10-IS2-02	文件管理程序書	限閱				110.03.31	1.2
			NTUCC-AC10-IS4-011	文件調閱申請單	限閱	109.09.18	1.1
			NTUCC-AC10-IS4-012	ISO 27001 文件管理列表	限閱	109.09.18	1.1
			NTUCC-AC10-IS4-166	ISO 9001 文件管理列表	一般	109.06.11	01
NTUCC-AC10-IS2-03	資訊資產管理程序書	限閱				109.09.18	1.3
			NTUCC-AC10-IS4-021	資訊資產清單	限閱	109.09.18	1.1
NTUCC-AC10-IS2-04	風險管理程序書	限閱				110.03.31	1.1
			NTUCC-AC10-IS4-026	風險評鑑報告	限閱	104.10.21	1.0
			NTUCC-AC10-IS4-027	適用性聲明書	限閱	109.09.18	1.3
			NTUCC-AC10-IS4-028	風險處理報告	限閱	104.12.02	1.0
			NTUCC-AC10-IS4-029	風險列表	限閱	108.10.14	1.0
			NTUCC-AC10-IS4-030	風險管理 KPI	限閱	104.10.26	1.0

8.執行紀錄

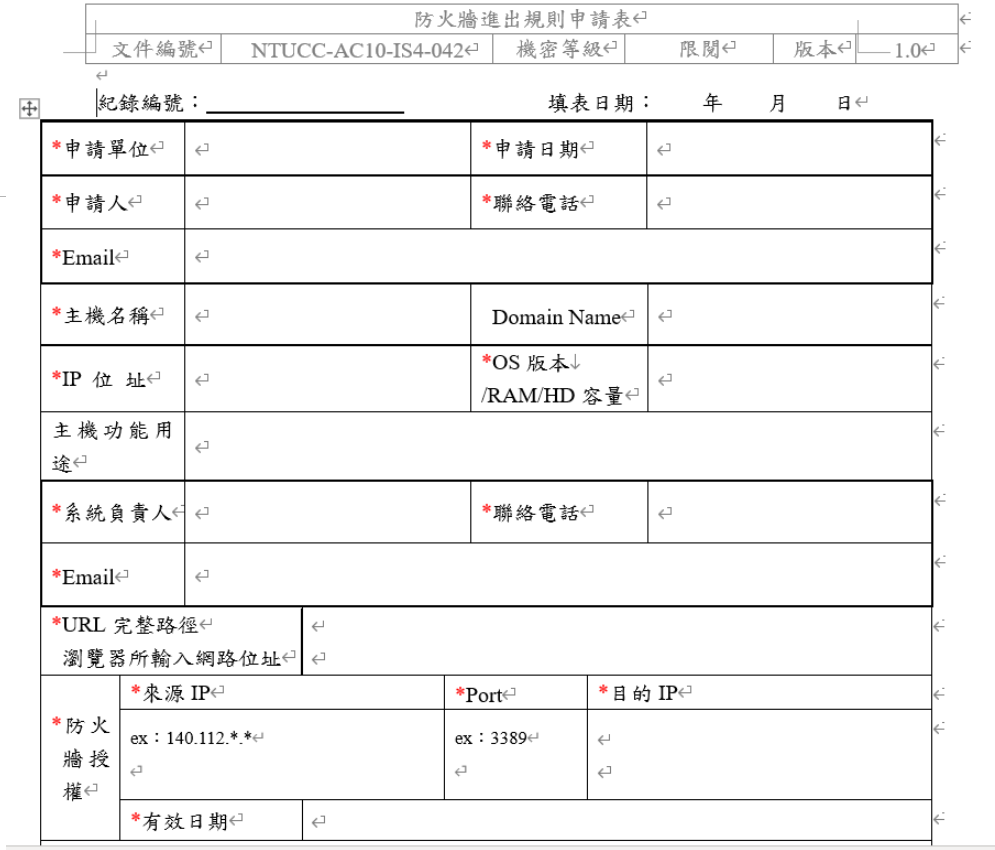
人員帳號異動清冊

文件編號	NTUCC-AC10-IS4-039	機密等級	限閱	版本	1.1

紀錄編號：_____ 填表日期： 年 月 日

系統/主機/資料夾名稱	帳號類型	帳號名稱	處理方式	交接者/承辦人	完成時間
□系統_____ □資料庫_____ □主機/資料夾_____ □防火牆帳號	□個人帳號 □管理者帳號	□ _____ □詳如電子檔	□刪除/停用帳號 □更改密碼 □移交作業程序		
□系統_____ □資料庫_____ □主機/資料夾_____ □防火牆帳號	□個人帳號 □管理者帳號	□ _____ □詳如電子檔	□刪除/停用帳號 □更改密碼 □移交作業程序		

1. 請詳列所管理帳號，處理原則：個人使用帳號於離職日刪除，系統帳號於完成交接後更改密碼，密碼設置需符合本中心 NTUCC-AC10-IS3-01 人員資訊安全守則規範。
2. 帳號名稱：若資料欄位量過多（如帳號數量眾多、密碼繁雜、處理方式繁複等），可採用電子檔方式交接。



防火牆進出規則申請表

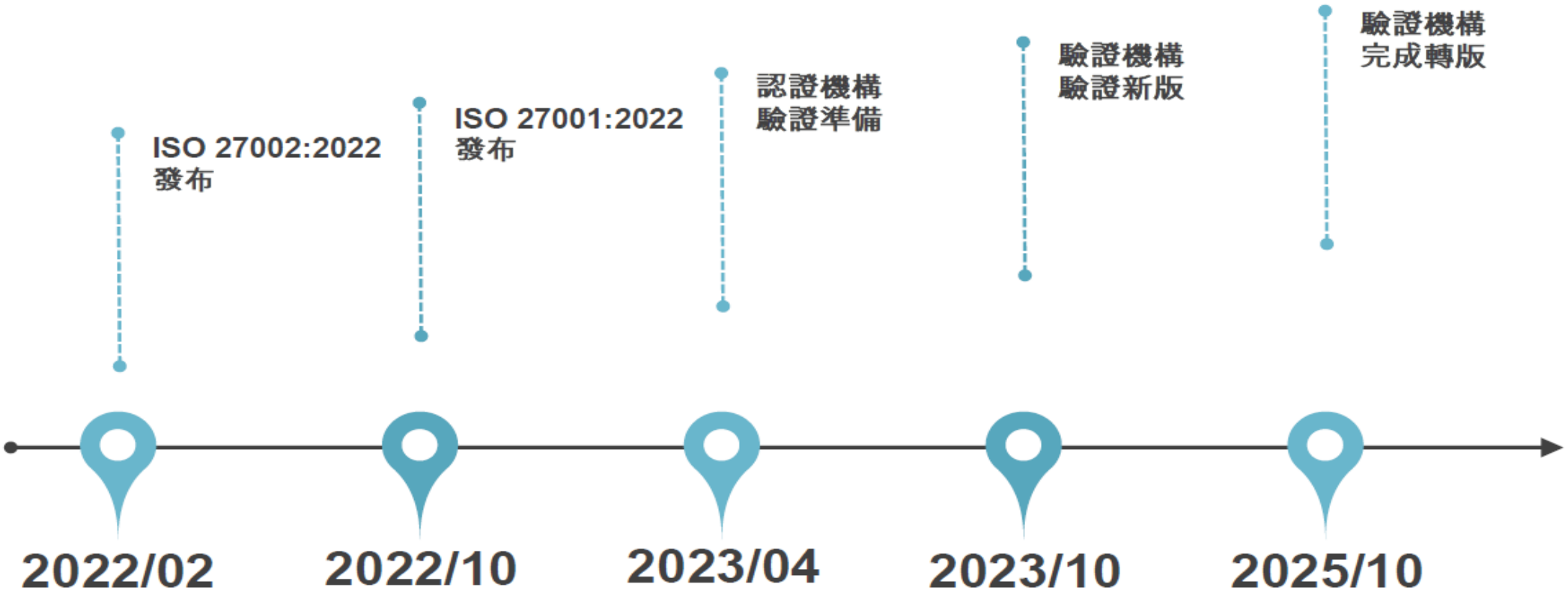
文件編號	NTUCC-AC10-IS4-042	機密等級	限閱	版本	1.0

紀錄編號：_____ 填表日期： 年 月 日

*申請單位		*申請日期	
*申請人		*聯絡電話	
*Email			
*主機名稱		Domain Name	
*IP 位 址		*OS 版本/RAM/HD 容量	
主機功能用途			
*系統負責人		*聯絡電話	
*Email			
*URL 完整路徑 瀏覽器所輸入網路位址			

*防火牆授權	*來源 IP	*Port	*目的 IP
	ex：140.112.*.*	ex：3389	
	*有效日期		

9.轉版驗證


ISO 27002:2022
發布
ISO 27001:2022
發布
認證機構
驗證準備
驗證機構
驗證新版
驗證機構
完成轉版
2022/02
2022/10
2023/04
2023/10
2025/10

10.持續改善

新版ISO27001效益

- 保護所有形式的資訊，包括紙本、雲端和數位資訊
- 提高抵禦網路攻擊的能力
- 提供集中管理的框架，在同一架構保護所有資訊
- 確保組織範圍內的保護，包括防護基於技術的風險和其他威脅
- 應對不斷演變的安全威脅
- 減少無效防護技術的成本和支出
- 保護完整性、機密性和可用性

為應對全球網路安全挑戰並提高數位信任度，發布了新的改進版本ISO/IEC 27001 。世界上最著名的資訊安全管理標準可幫助組織保護其資訊資產，在當今日益數位化的世界中至關重要。

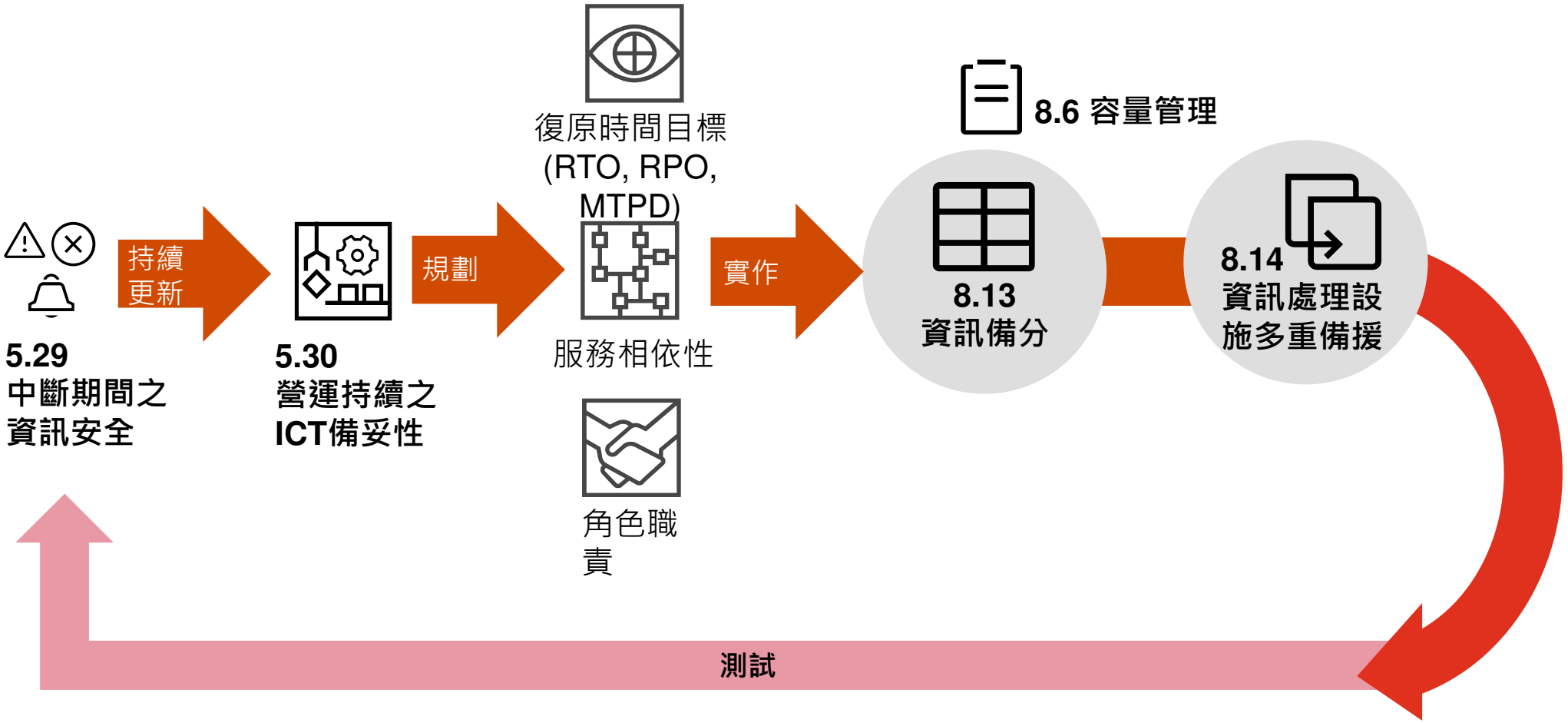
隨著駭客開發出更先進的網路犯罪技術，網路犯罪變得越來越嚴重和復雜。世界經濟論壇的 《 全球網路安全展望 》報告顯示， 2021 年全球網路攻擊增加了 125%，有證據表明到 2022 年將持續上升。在這個瞬息萬變的環境中，領導者必須提升戰略方法應對網路風險。

當您使用ISO/IEC 27001 時，您向利害關係者和客戶證明您致力於安全可靠地管理資訊。這是宣傳您的組織、慶祝您的成就並證明您值得信賴的好方法。

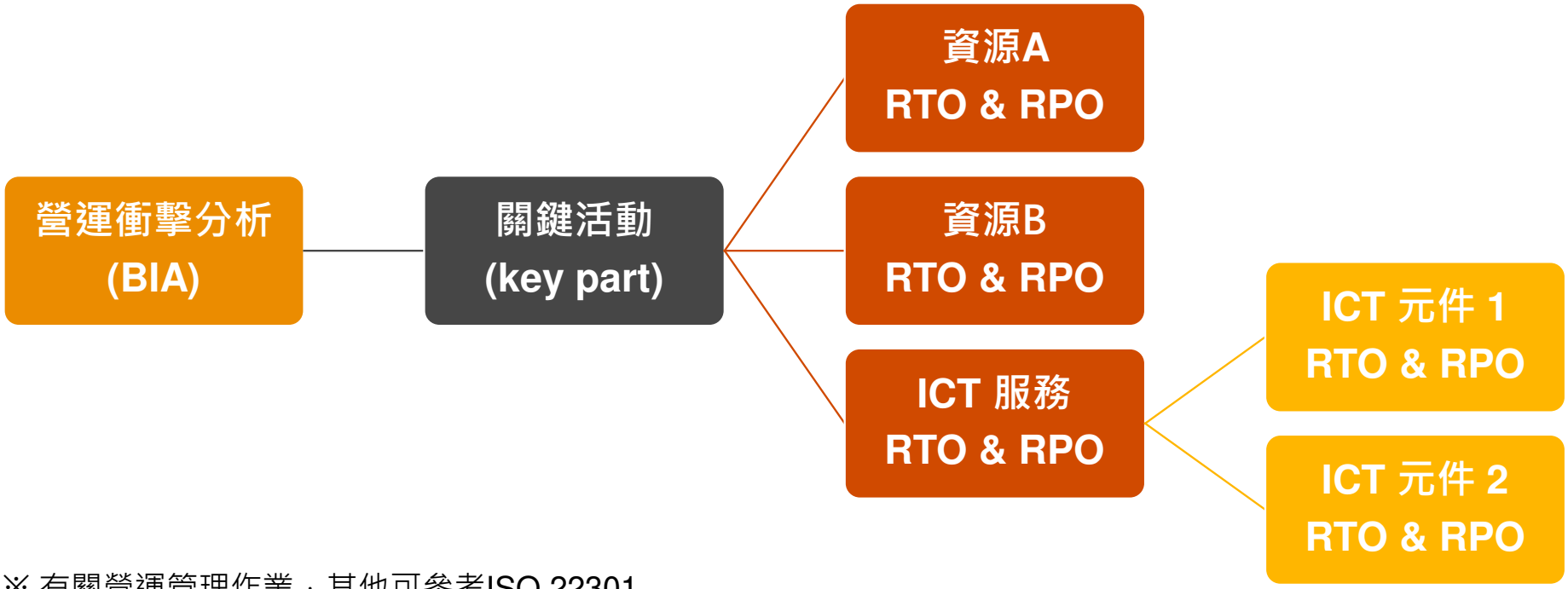
4

新版ISO27001控制措施要求綜合說明(打通任督二脈)

#Continuity 持續性



#Continuity 持續性
資通訊技術(ICT)營運持續整備



※ 有關營運管理作業，其他可參考ISO 22301

#Physical Security 實體安全

實體安全監視 Physical security monitoring

持續監控

- 實體場域宜由監視系統進行監控，包括：警衛、入侵警報、CCTV 、實體環境管理系統...等。

監控範圍

- 宜持續監視建置有關鍵系統的建築物其進出存取，以偵測未經授權的進出或可疑行為。

監控強度

- 持續監控並能追溯查看；具備入侵偵測與警報； 防竄改與持續運作機制。

#Application Security 應用程式安全

安全程式碼撰寫 Secure coding

撰寫前規劃

應備有系統安全開發之程式碼撰寫原則，以供公司內部及供應商遵循，其內容應包含：

- 組織准許之例外
- 常見的資訊安全漏洞
- 配置之開發工具及執行環境維護及使用
- 開發人員資格
- 安全設計及架構

撰寫中

- 使用安全程式碼撰寫技術
- 使用結構化編程技術

檢視並維護

- 處理發現之安全漏洞
- 保護程式碼不受到未經授權的存取
- **使用程式碼掃描工具**

  確保所使用之程式庫、組件、軟體等是否安全並經過核可，且已定期更新至最新版本

當ISO 27001 修改後，我們應該...

確認組織政策有包含所有93個新的控制措施(包含工具的導入)

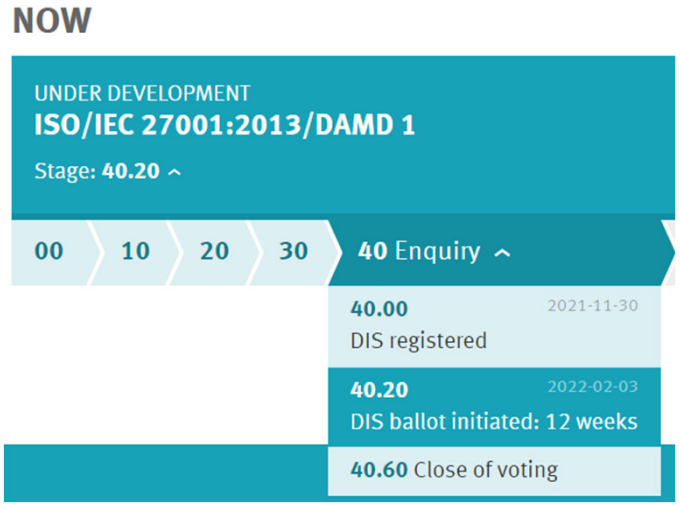
更新組織政策與程序

更新適用性聲明

更新監控計畫

更新內部稽核計畫與報告模板

在規範的時限內完成更新



Thank you

pwc.tw