ISO27002 資訊安全實務指導規範之新版初探

八月 2022

pwc 資誠

Agenda

1. ISO 27001新版預計改版方向說明
2. ISO 27002:2022 資訊安全實務指導規範新增項目介紹

講師介紹 – 黃承漢 Michael Huang

- 經歷
- PwC 資誠聯合會計師事務所 風險及控制服務 經理
- PwC 資誠聯合會計師事務所 資訊安全暨鑑識科技實驗室品質負責人
- PwC 資誠聯合會計師事務所 風險及控制服務 資深顧問
- PwC 資誠企業管理顧問股份有限公司 資深顧問
- 華碩電腦 電腦中心策略規劃室 IT運營專案課 資安工程師
- 曜揚科技 技術服務部組長

專業證照

- PMP(Project Management Professional)國際專案管理師認證
- EC-Council CHFI 資安鑑識調查專家認證
- ISO27001:2005及2013 LA; ISO29100:2011 LA ; BS10012: 2009 及2017 LA
- ISO27018 :2014 LA; ISO27701: 2019 LA ; ISO22301: 2019 LA ;
- ISO27025 :2017資安實驗室主管驗證訓練合格
- SGS「資通系統防護基準–合規技術專員」證書
- ITIL v3 Foundation 認證
- TCSE（ Trend Certified Security Expert 趨勢認證資訊安全專家 ）
- 微軟MCTS(Hyper-V 虛擬化解決方案)
- 微軟MCTS(Exchange)
- 微軟MCTS(SharePoint , Configuring)
- 中華數位SPAM SQR專業證照

ISO 27001新版預計改版方向說明

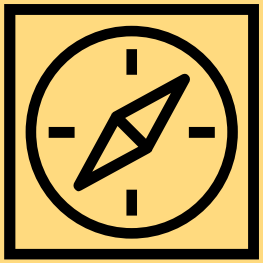
ISO 國際標準介紹

創立於於 1946 年

總部設在瑞士日內瓦

平均每五年檢討標準一次

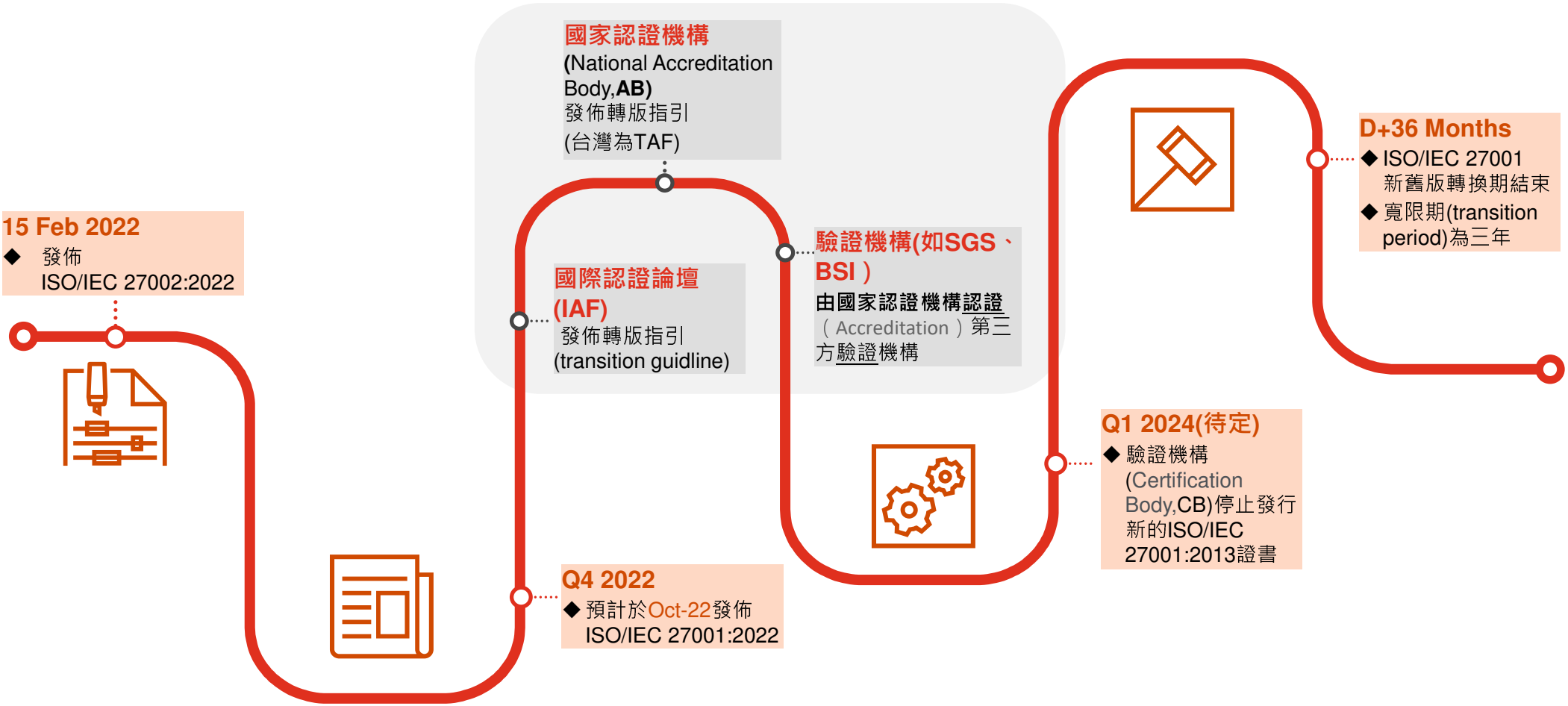
總共有 167 個會員國



主要宗旨為促進國際合作，負責制定在全球通用的國際標準，以 推動國際交流，國際貿易和科學技術的發展，加強國際間經濟合作通道。

ISO 國際標準修改流程

ISO/IEC 27001:2022預計轉版時程

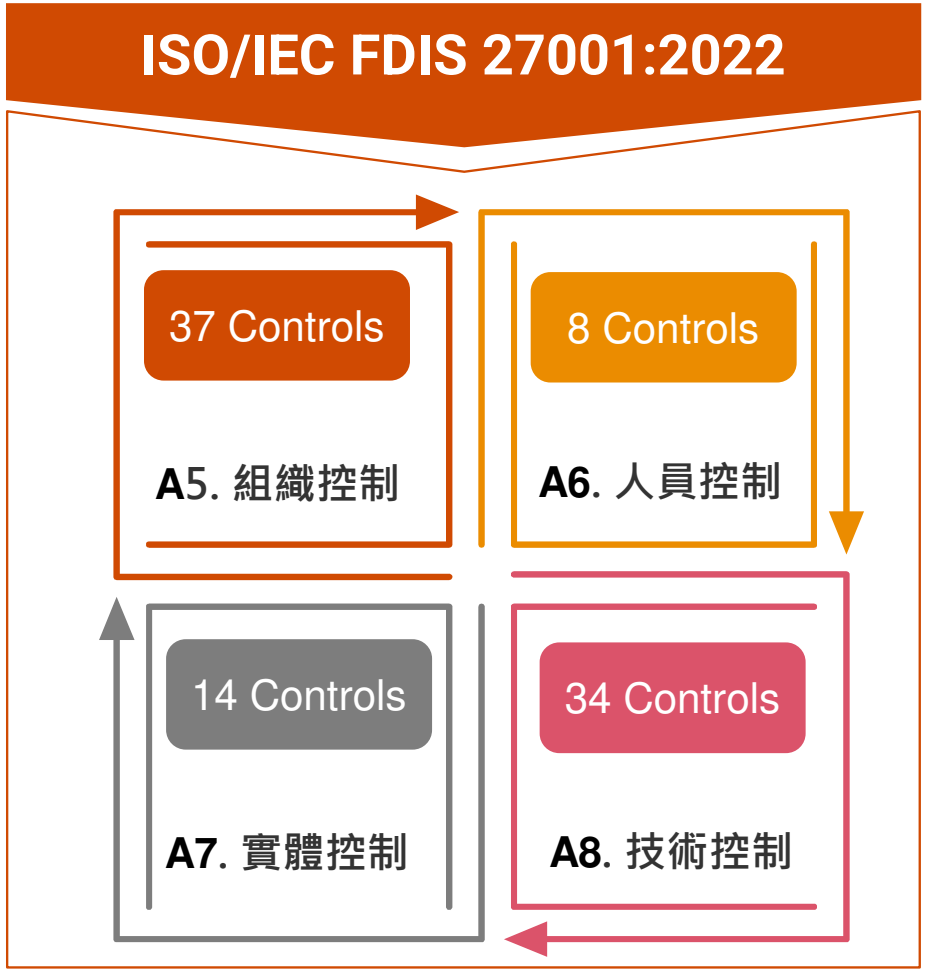


控制類別

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



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
茲舉部分範例於後附投影片

ISO/IEC
27001:2013

茲舉部分範例於
後附投影片

ISO/IEC
FDIS 27001

整併之控制項目(部分舉例)
24 Merged Controls

- A.6.1.5

專案管理之資訊安全

- A.14.1.1

資訊安全要求事項分析及規格

A5.8
專案管理的資訊安全

- A.13.2.1

資訊傳送政策及程序

- A.13.2.2

資訊傳送協議

- A.13.2.3 電子傳訊

A5.14
資訊傳送

- A.9.2.4

使用者之秘密鑑別資訊的管理

- A.9.3.1

秘密鑑別資訊之使用

- A.9.4.3 通行碼管理系統

A5.17
驗證資訊

- A.8.1.3

資產之可被接受使用

- A.8.2.3

資產之處置

A5.10
使用資訊及相關聯資產

重命名之控制項目(部分舉例)
23 Renamed Controls

	A.9.2.1 使用者註冊及註銷	1	A.5.16 身分管理
	A.18.1.4 個人可識別資訊之隱私及保護 Privacy and protection of personally identifiable information	2	A.5.34 個人可識別資訊之隱私及保護 Privacy and protection of PII
	A.6.2.2 遠距工作 Teleworking	3	A.6.7 遠距工作 Remote working
	A.9.4.2 保全登入程序	4	A.8.5 安全認證
	A.17.2.1 資訊處理設施之可用性	5	A.8.14 資訊處理設施之多重備援 Redundancy of information processing facilities
	A.14.3.1 測試資料之保護 Protection of test data	6	A.8.33 測試資料之保護 Test information

ISO 27002:2022 資訊安全實務指導規範新增項目介紹

從27002改版透析27001走向

ISO/IEC 27002:2013

Information technology — Security techniques — Code of practice for information security controls

資訊科技— 安全技術 — 資訊安全控制措施之作業規範

標準名稱修改

ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection — Information security controls

資訊安全、網路安全和隱私保護——資訊安全控制

從27002改版透析27001走向

5. 組織控制
37 控制項

6. 人員控制
8 控制項

7. 實體控制
14 控制項

8. 技術控制
34 控制項

114 項
控制措施
14 類

80頁

93 項
控制措施
4 類

152頁

修改數量

- ◆ 23個控制項目重新命名
- ◆ 多個控制項目併為24個控制項目
- ◆ 新增加的控制項目
- ◆ 35個修改編號

新增及修改之說明欄

27002:2013	27002:2022
• 無定義 (Not defined)	• 控制標題 (Control title)
	• **屬性表格 (Attribute table)**
• 控制 (Control)	• 控制 (Control)
	• **目標 (Purpose)**
• 實作指引 (Implementation guidance)	• 指引 (Guidance)
• 其他資訊 (Other Information)	• 其他資訊 (Other Information)

27002新增5個屬性標籤

屬性名稱	說明	範例
控制類型	控制如何影像資訊安全事故發生時的風險結果	#預防性、#偵測性、#矯正性...
資安特性	常見特性C、I、A	#機密性、#完整性、#可用性...
網路安全概念	符合ISO27001中定義的網路安全架構	#識別、#保護、#偵測、#回應、#復原...
執行能力	15個分類標籤，涵蓋控制安全分類的廣泛視角	#治理、#資產管理...
安全領域	資訊安全的不同領域	#防禦、#保護...

範例

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.1	Policies for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

27002增加11個控制項目 – 組織控制

威脅情資
(Threat intelligence)

雲端服務使用的資安
(Information security for use of cloud services)

資通訊技術營運持續整備
(ICT readiness for business continuity)

27002增加11個控制項目 – 實體控制

實體安全監控
(Physical security monitoring)

27002增加11個控制項目 – 技術控制

組態管理
(Configuration management)

資訊刪除
(Information deletion)

資料遮罩
(Data masking)

資料外洩防護
(Data leakage prevention)

活動檢視
(Monitoring activities)

網站過濾
(Segregation of networks)

安全程式碼撰寫
(Secure coding)

增加的控制項目- 5.7威脅情資(Threat intelligence)

Control：

應收集和分析與資訊安全威脅有關的資訊，以產生威脅情資。

Purpose：

提供對組織威脅環境的意識，以便可以採取適當的緩解措施。

與ISO27001:2013年的要求對應:

- ISO 27001:2013主條文外部議題
- 資安事故的學習(與證據之搜集)
- 事件存錄（log)
- 資通安全管理法-資通安全情資分享
- 與特殊關係方之聯繫

增加的控制項目- 5.23雲端服務使用的資訊安全
(Information security for use of cloud services)

Control：

應根據組織的資訊安全要求，建立獲取、使用、管理和退出雲服務的流程。

Purpose：

指定並管理使用雲服務的資訊安全性。

與ISO27001:2013年的要求對應:

- 網路控制措施、供應商關係

亦可參閱：

- ISO 17788、ISO 17789、ISO 22123、ISO 19941、ISO 27017、ISO 27018、ISO 27036、ISO 19086

增加的控制項目- 5.30資通訊技術營運持續整備(ICT readiness for business continuity)

Control：

資通訊技術整備應根據業務連續性目標和資通訊技術連續性要求，進行規劃、實施、維護和測試。

Purpose：

確保在中斷期間組織的資訊和其他相關資產的可用性。

與ISO27001:2013年的要求對應:

- 規劃資訊安全營運持續
- 通報資訊安全事件
- 查證、審查並評估資訊安全持續

亦可參閱：

- ISO 27031、ISO 22301、ISO 22313

增加的控制項目- 7.4實體安全監控(Physical security monitoring)

Control：

應持續監測作業場所是否存在未經授權的實體進出。

Purpose：

偵測和阻止未經授權的實體進出。

與ISO27001:2013年的要求對應:

- 設備安置及保護
- 無人看管之使用者設備
- 使用者存取權限之審查

增加的控制項目- 8.9組態管理(Configuration management)

Control：

應建立、記錄、實施、監控和審查硬體、軟體、服務和網路的配置，包括安全配置。

Purpose：

確保硬體、軟體、服務和網路在所需的安全設置下正常運行，並且配置不會因未經授權或不正確的更改而改變。

與ISO27001:2013年的要求對應:

- 變更管理
- 資訊備份
- 文件化資訊的控制
- 紀錄之保護
- 保全系統工程原則
- 系統變更控制程序
- 運作平台變更後之應用的技術審查

增加的控制項目- 8.10資訊刪除(Information deletion)

Control：

當不再需要時，應刪除儲存在資訊系統、設備或任何其他存儲媒體中的資訊。

Purpose：

防止敏感資訊不必要的暴露，並遵守有關資訊刪除的法律、法令、法規和合約要求。

與ISO27001:2013年的要求對應:

- A.8.3.2 媒體之汰除
- A.8.2.3 資產之處置
- A.8.3.1 可移除式媒體之管理
- A.11.2.7 設備汰除或再使用之保全

與相關要求對應:

- 個資法: 個資依保留週期刪除
- ISO27701:2019中 PII 暫存檔的處置

增加的控制項目- 8.11資料遮罩(Data masking)

Control：

資料遮蔽應根據組織的特定主題存取控制政策和其他相關特定主題政策和業務需求使用，並考慮適用的法規。

Purpose：

限制敏感資料（包括 個資(PII)）的暴露，並遵守法律、法令、法規和合約要求

與ISO27001:2013年的要求對應:

- A.14.3.1 測試資料之保護
- A.18.1.4 個人可識別資訊之隱私及保護

與ISO27701:2019年的要求對應:

- 個資處理後的去識別化與刪除
- 個資最小化的目標
- 預設隱私的保護與設計

增加的控制項目- 8.12資料外洩防護(Data leakage prevention)

Control：

資料外洩的預防措施應應用於處理、存儲或傳輸敏感資訊的系統、網絡和任何其他設備。

Purpose：

偵測和防止個人或系統未經授權揭露和擷取資訊。

與ISO27001:2013年的要求對應:

- A.13.2.3 電子傳訊
- A.13.1.1 網路控制措施
- A.13.1.3 網路之區隔
- A. 8.3.1 可移除式媒體的管理
- A.6.2.1 行動裝置政策
- A.12.4.1 事件存錄
- A.12.4.3 管理者及操作者日誌

增加的控制項目- 8.16活動檢視(Monitoring activities)

Control：

應監控網路、系統和應用程序的異常行為，並採取適當措施評估潛在的資訊安全事件。

Purpose：

檢測異常行為和潛在的資訊安全事件。

可參考以下方式增強監控：

- 利用威脅情資系統
- 利用機器學習和人工智慧能力;
- 使用黑名單或白名單;
- 進行一系列技術安全評估，確定基線Baseline或可接受的行為;
- 使用監控系統，建立和檢測異常行為;
- 管理者及操作者日誌存錄與保護

增加的控制項目- 8.23網站過濾(Web filtering)

Control：

應管理對外部網站的存取，以減少暴露於惡意內容。

Purpose：

保護系統免受惡意軟體的入侵，並防止存取未經授權的網站資源。

與ISO27001:2013年的要求對應:

- 對網路及網路服務之存取
- 網路服務之安全

增加的控制項目- 8.28安全程式碼撰寫(Secure coding)

Control：

安全程式編碼原則應應用於軟體開發。

Purpose：

確保軟體編寫安全，從而減少軟體中潛在資訊安全漏洞的數量。

與相關要求對應:

- ISO27001:2013保全系統工程原則、系統安全測試、技術脆弱之管理、保全開發政策
- ISO27701:2019 PII 處理後的去識別化與刪除、最小化的目標、預設隱私的保護與設計
- BSIMM Attack Models
- 資安事件/事故回饋
- 官方SDK 的 Secure API

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)

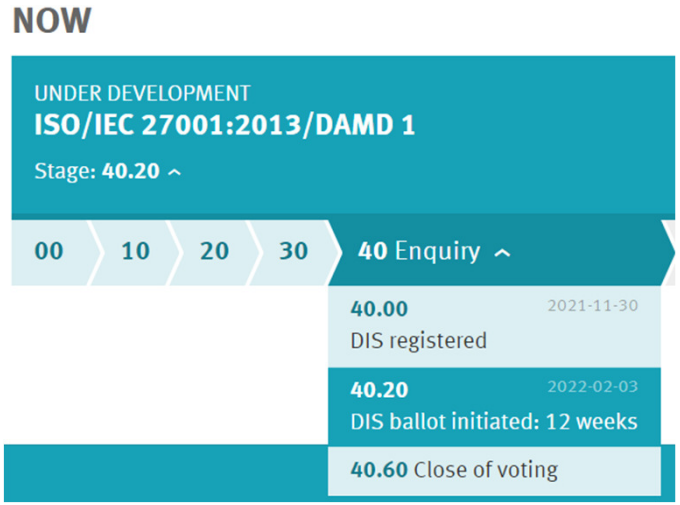
更新組織政策與程序

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

黃承漢 經理

(02) 2729 6666 ext.23227 **michael.a.huang@pwc.com**