數位轉型時代的資訊安全
新版ISO 27001重點解析

Gaia Security Consultant , 王艾敏 Amy Wang

蓋亞資訊有限公司
雲端服務整合專家
Bridge you to the world with our expertise.
2024/02/22

GAIA Information Technology

WHO ARE WE

台灣最專業的雲端資安廠商與亞太區最大 Anti-DDoS 供應商

Kubernetes 台灣第一家通過 CNCF 認證之混合雲供應商與講師

全方位一站式雲端整合顧問服務

24hr 中英雙語線上維運服務

代理數十個國際品牌、服務上千家企業

Agenda

- 資安趨勢及相關法規
- ISO 27001:2022變動概要說明
- 新版控制措施之調整說明
- 新版實作常見問題

GAIA Information Technology

資安趨勢及相關法規

資安新聞-詐騙再進化，視訊會議也能偽冒！

示意圖。（圖取自Unsplash圖庫）

16 讚

（中央社香港4日綜合外電報導）香港發生首宗運用深偽技術企業詐騙案，騙徒假冒一間跨國公司英國總部財務長，透過視訊會議要求香港分公司財務部門職員轉帳15次，共騙走約港幣2億元（約新台幣8億元）。

假財務長深偽視訊會議 跨國公司香港分部被騙8億

- 歹徒運用**深偽技術（Deepfake）**，偽冒跨國公司英國總部財務長身份
- **假冒公司高階主管召開視訊電話會議**，要求財務部職員對指定銀行帳戶匯款
- 相關深偽影片事先錄製，視訊會議期間**沒有跟被害人進行交談或互動**
- 多人參與那場視訊會議，但除了該名被害人之外，其他人都是假冒的
- 被害人轉帳15次，匯出約港幣2億元（**約台幣8億元**）

新聞來源：中央社https://www.cna.com.tw/news/aopl/202402050004.aspx

資安新聞-安全的開發環境與員工意識很重要！

賓士員工 GitHub 的 Token 不慎公開，恐導致其原始碼外流

開發人員若是不慎將自己的Token曝露在網際網路上，有可能導致所屬企業也跟著受害，最近有資安業者發現汽車大廠賓士（Mercedes-Benz）資料外洩的情況，起因就是員工在程式碼儲存庫GitHub曝露這類資料

文/ 周峻佑 | 2024-02-02 發表

讚 152 分享

- 資安業者網路掃描中發現賓士不慎洩露員工的身份驗證 Token
- 一旦取得，就能對賓士自行管理的 GitHub Enterprise Server **完整存取其中的原始碼**
- 程式碼儲存庫包含**大量智慧財產**，以及**資料庫連線資訊**、雲端服務存取金鑰、**設計圖**、**設計文件**、單一簽入（SSO）**密碼**、API 金鑰，以及其他重要的內部訊息

資料來源：IThome https://www.ithome.com.tw/news/161173

工程會與數發部「政府資訊服務採購作業指引」

各類資訊（服務）採購之共通性資通安全基本要求參考一覽表

應用軟體或系統開發服務

類型		項目	子項	資料或系統類型 高	中	普	說明
		提供服務商	具備完善之資通安全管理措施	●	●	●	1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級（高、中、普），並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
			須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	◎	
			須具備IEC 62443 資安檢測實驗室（CBTL）資格	◎	◎	◎	
			須具備發佈CVE的資格及能力	◎	◎	◎	
			開發系統導入安全軟體發展生命週期(Secure Software Development Life Cycle, SSDLC)	◎	◎	◎	
			不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	
		符合國際標準規範	協助系統導入及取得CNS27001及ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準驗證	◎	◎	◎	

雲端微服務（SaaS）辦公室生產力工具（含郵件、行事曆、雲端硬碟、即時通訊等）

類型		項目	子項	資料或系統類型 高	中	普	說明
		提供服務商	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	●	1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級（高、中、普），並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
			須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準	◎	◎	◎	提供服務項目涉及個資時應納入要求。
			不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
		傳輸機密性與完整性	廠商提供機關資料傳輸措施	●	●	●	
		事件日誌保存與可歸責性	應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求	●	●	●	

資料來源：行政院工程會
https://planpe.pcc.gov.tw/prms/explainLetter/readPrmsExplainLetterContentDetail?pkPrmsRuleContent=7500 1760&_csrf=41c91031-1b1a-45e1-8814-ff2f59c93227

上市櫃公司須遵守之資安規定

- 公開發行公司建立內控制度處理準則

- 上市櫃公司資通安全管控指引

政策及管理面	技術面	認知訓練
• 成立資安推動組織與制定資安目標 • 設立資安專責人員 • 裝置使用管理規範 • 資訊作業委外安全管理程序 • 內部資安稽核 • 業務持續演練、備份機制及備援計畫 • 鑑別應遵守之法令及契約要求 • 資產盤點及風險評估 • 資安事件應變處置及通報作業程序	• 資安要求納入系統開發及維護需求規格 • 定期安全性檢測並完成系統弱點修補 • 資安威脅偵測管理 • 資安防護與控制 • 實體安全控管	• 資安教育訓練 • 資安專業課程訓練 • 每年定期辦理電子郵件社交工程演練

資料來源：臺灣證券交易所

112.05.31新版個人資料保護法

2023《個人資料保護法》部分條文修正，罰則大幅提高！

Before

- 非公務機關若未採行適當安全措施來防止個資被竊、竄改、 ....，限期改正，屆期未改正者，按次處新台幣**2萬元以上20萬元以下罰鍰**

2023.05.16

《個人資料保護法》部分條文修正案三讀通過

After

- **主管機關為「個人資料保護委員會」**
- 修正個資法第48條，非公務機關若未採行適當安全措施來防止個資被竊、竄改....，情節重大者，處**15萬元以上1,500萬元以下罰鍰**；屆期未改正者，按次處15萬元以上1,500萬元以下罰鍰。

ISO 27001 變動概要說明

ISO 27001標準名稱調整

【2013版】

- 資訊科技-安全技術-資訊安全管理系統-要求
- Information technology-Security techniques -Information security management systems –Requirements

【 2022版】

- 資訊安全-網宇安全及隱私保護-資訊安全管理系統-要求
- Information Security, Cybersecurity and Privacy Protection -Information security management systems –Requirements

ISO 27001主條文異動

主條文 – 新增	
6.3	變更之規劃
9.2.1	概述 (內部稽核)
9.2.2	內部稽核方案
9.3.1	概述 (管理審查)
9.3.2	管理審查輸入
9.3.3	管理審查輸出

主條文 – 新增文字	
4.2	瞭解關注方之需要及期望
4.4	資訊安全管理系統
6.2	資訊安全目標及達成之規劃
7.4	溝通
8.1	運作之規劃及控制
9.1	監督、量測、分析及評估
9.3.2	管理審查輸入

主條文 – 異動	
4.1	瞭解組織及其全景
5.1	領導及承諾
5.3	組織角色、責任及權限
6.1.3	資訊安全風險處理
8.1	運作之規劃及控制
9.1	監督、量測、分析及評估
9.2.2	內部稽核方案
9.3.3	管理審查輸出

主條文 – 順序對調	
10.1	持續改善
10.2	不符合項目及矯正措施

附錄 A 及相關之 ISO 27002 版變化

- **新版控制要求的內容有大幅變動與新增。**

- **控制措施從目前的 114 個減少到 93 個控制措施。**
  - ISO/IEC 27002：2013 包含 114 項控制措施，分為 14 類。
  - **ISO/IEC 27002：2022 包含 93 項控制，分為 4 類：**
    1. 組織控制 - 37項
    2. 人員控制 - 08項
    3. 實體控制 - 14項
    4. 技術控制 - 34項
  - 更新58個控制項目，將多個控制項目併為24個控制項目，並新增11個控制項目。

新版控制措施之調整說明

附錄 A 新增之控制措施（新增11項）

編號	項目名稱	控制措施
5.7	威脅情資	應收集及分析與資訊安全威脅相關的資訊，以產出威脅情資。
5.23	使用雲端服務之資訊安全	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。
5.30	資通訊技術營運持續整備	應根據營運持續目標和 ICT 持續性要求來規劃、實施、維護和測試 ICT 整備情況。
7.4	實體安全監視	應持續監控場域周界以防止未經授權的實體存取。
8.9	組態管理	應建立、文件化、實作、監視和審查硬體、軟體、服務和網路的組態，包括安全組態。
8.10	資訊刪除	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。
8.11	資料遮蔽	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。
8.12	預防資料洩漏	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。
8.16	監視活動	應監視網路、系統和應用程序的異常行為並 採取適當的措施來評估潛在的資訊安全事故。
8.22	網頁過濾	應管理對外部 網站的存取，以減少曝露於惡意的內容。
8.28	安全程式設計	軟體開發應採用安全編碼原則。

附錄 A 新增之控制措施（新增11項）

編號	項目名稱	控制措施
5.7	威脅情資	應收集及分析與資訊安全威脅相關的資訊，以產出威脅情資。
5.23	使用雲端服務之資訊安全	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。
5.30	資通訊技術營運持續整備	應根據營運持續目標和 ICT 持續性要求來規劃、實施、維護和測試 ICT 整備情況。
7.4	實體安全監視	應持續監控場域周界以防止未經授權的實體存取。
8.9	組態管理	應建立、文件化、實作、監視和審查硬體、軟體、服務和網路的組態，包括安全組態。
8.10	資訊刪除	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。
8.11	資料遮蔽	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。
8.12	預防資料洩漏	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。
8.16	監視活動	應監視網路、系統和應用程序的異常行為並 採取適當的措施來評估潛在的資訊安全事故。
8.22	網頁過濾	應管理對外部 網站的存取，以減少曝露於惡意的內容。
8.28	安全程式設計	軟體開發應採用安全編碼原則。

附錄 A 新增之控制措施（新增11項）

編號	項目名稱	控制措施
5.7	威脅情資	應收集及分析與資訊安全威脅相關的資訊，以產出威脅情資。
5.23	使用雲端服務之資訊安全	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。
5.30	資通訊技術營運持續整備	應根據營運持續目標和 ICT 持續性要求來規劃、實施、維護和測試 ICT 整備情況。
7.4	實體安全監視	應持續監控場域周界以防止未經授權的實體存取。
8.9	組態管理	應建立、文件化、實作、監視和審查硬體、軟體、服務和網路的組態，包括安全組態。
8.10	資訊刪除	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。
8.11	資料遮蔽	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。
8.12	預防資料洩漏	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。
8.16	監視活動	應監視網路、系統和應用程序的異常行為並 採取適當的措施來評估潛在的資訊安全事故。
8.22	網頁過濾	應管理對外部 網站的存取，以減少曝露於惡意的內容。
8.28	安全程式設計	軟體開發應採用安全編碼原則。

附錄 A 新增之控制措施（新增11項）

編號	項目名稱	控制措施
5.7	威脅情資	應收集及分析與資訊安全威脅相關的資訊，以產出威脅情資。
5.23	使用雲端服務之資訊安全	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。
5.30	資通訊技術營運持續整備	應根據營運持續目標和 ICT 持續性要求來規劃、實施、維護和測試 ICT 整備情況。
7.4	實體安全監視	應持續監控場域周界以防止未經授權的實體存取。
8.9	組態管理	應建立、文件化、實作、監視和審查硬體、軟體、服務和網路的組態，包括安全組態。
8.10	資訊刪除	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。
8.11	資料遮蔽	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。
8.12	預防資料洩漏	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。
8.16	監視活動	應監視網路、系統和應用程序的異常行為並 採取適當的措施來評估潛在的資訊安全事故。
8.22	網頁過濾	應管理對外部 網站的存取，以減少曝露於惡意的內容。
8.28	安全程式設計	軟體開發應採用安全編碼原則。

附錄 A 新增之控制措施（新增11項）

編號	項目名稱	控制措施
5.7	威脅情資	應收集及分析與資訊安全威脅相關的資訊，以產出威脅情資。
5.23	使用雲端服務之資訊安全	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。
5.30	資通訊技術營運持續整備	應根據營運持續目標和 ICT 持續性要求來規劃、實施、維護和測試 ICT 整備情況。
7.4	實體安全監視	應持續監控場域周界以防止未經授權的實體存取。
8.9	組態管理	應建立、文件化、實作、監視和審查硬體、軟體、服務和網路的組態，包括安全組態。
8.10	資訊刪除	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。
8.11	資料遮蔽	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。
8.12	預防資料洩漏	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。
8.16	監視活動	應監視網路、系統和應用程序的異常行為並 採取適當的措施來評估潛在的資訊安全事故。
8.22	網頁過濾	應管理對外部 網站的存取，以減少曝露於惡意的內容。
8.28	安全程式設計	軟體開發應採用安全編碼原則。

附錄 A 新增之控制措施（新增11項）

編號	項目名稱	控制措施
5.7	威脅情資	應收集及分析與資訊安全威脅相關的資訊，以產出威脅情資。
5.23	使用雲端服務之資訊安全	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。
5.30	資通訊技術營運持續整備	應根據營運持續目標和 ICT 持續性要求來規劃、實施、維護和測試 ICT 整備情況。
7.4	實體安全監視	應持續監控場域周界以防止未經授權的實體存取。
8.9	組態管理	應建立、文件化、實作、監視和審查硬體、軟體、服務和網路的組態，包括安全組態。
8.10	資訊刪除	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。
8.11	資料遮蔽	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。
8.12	預防資料洩漏	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。
8.16	監視活動	應監視網路、系統和應用程序的異常行為並 採取適當的措施來評估潛在的資訊安全事故。
8.22	網頁過濾	應管理對外部 網站的存取，以減少曝露於惡意的內容。
8.28	安全程式設計	軟體開發應採用安全編碼原則。

附錄 A 新增之控制措施（新增11項）

編號	項目名稱	控制措施
5.7	威脅情資	應收集及分析與資訊安全威脅相關的資訊，以產出威脅情資。
5.23	使用雲端服務之資訊安全	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。
5.30	資通訊技術營運持續整備	應根據營運持續目標和 ICT 持續性要求來規劃、實施、維護和測試 ICT 整備情況。
7.4	實體安全監視	應持續監控場域周界以防止未經授權的實體存取。
8.9	組態管理	應建立、文件化、實作、監視和審查硬體、軟體、服務和網路的組態，包括安全組態。
8.10	資訊刪除	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。
8.11	資料遮蔽	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。
8.12	預防資料洩漏	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。
8.16	監視活動	應監視網路、系統和應用程序的異常行為並 採取適當的措施來評估潛在的資訊安全事故。
8.22	網頁過濾	應管理對外部 網站的存取，以減少曝露於惡意的內容。
8.28	安全程式設計	軟體開發應採用安全編碼原則。

A.5.7 威脅情資

編號	項目名稱	控制措施
5.7	威脅情資	應收集及分析與資訊安全威脅相關的資訊，以產出威脅情資。

- 善用威脅情資

相關
Relevant

與組織的保護有關。

情境化
Contextual

情資情境，例如：時間、地點、經驗、同產業狀況 ...

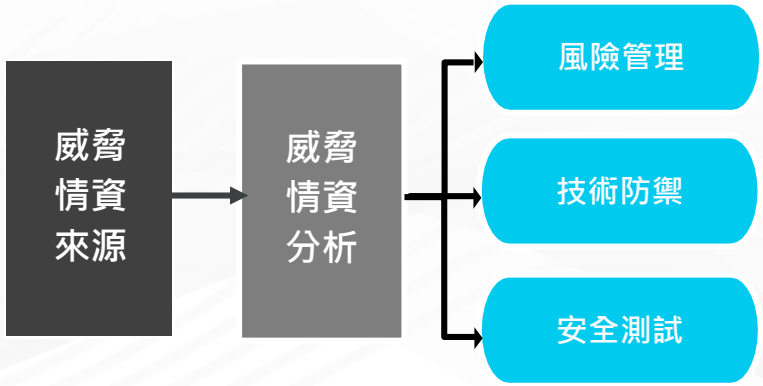
具洞察力
Insightful

為組織提供對威脅形勢的準確和詳細的了解。

可行動
Actionable

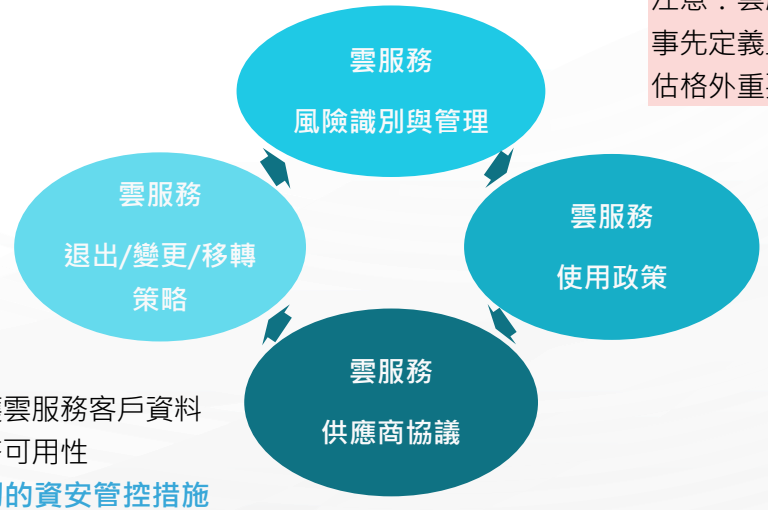
組織可以快速、有效地依據資訊採取行動。

- 有效威脅情資四大原則



A.5.23使用雲端服務之資訊安全

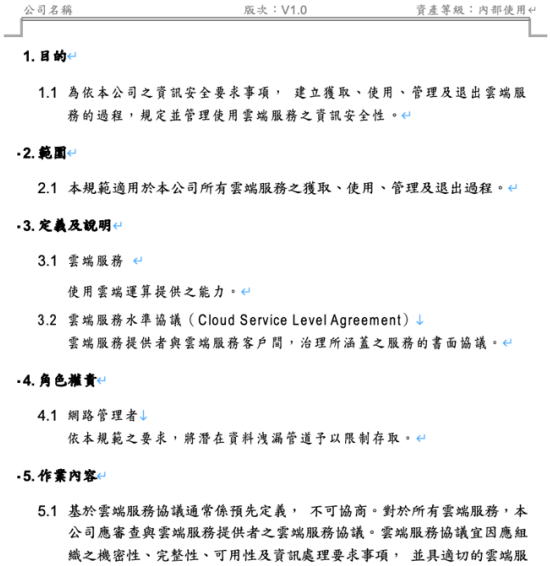
編號	項目名稱	控制措施
5.23	使用雲端服務之資訊安全	應根據組織的資訊安全要求建立獲取、使用、管理和退出雲端服務的流程。



- 保護雲服務客戶資料
- 服務可用性
- **適切的資安管控措施**

注意：雲服務協議或合約通常是事先定義且不接受協商，事前評估格外重要。

- **法令法規**
- 使用範圍
- **資安要求**
- **角色權責**
- .....等



公司名稱　　版次：V1.0　　資產等級：內部使用

1. 目的

1.1 為依本公司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，規定並管理使用雲端服務之資訊安全性。

2. 範圍

2.1 本規範適用於本公司所有雲端服務之獲取、使用、管理及退出過程。

3. 定義及說明

3.1 雲端服務

使用雲端運算提供之能力。

3.2 雲端服務水準協議（Cloud Service Level Agreement）

雲端服務提供者與雲端服務客戶間，治理所涵蓋之服務的書面協議。

4. 角色權責

4.1 網路管理者

依本規範之要求，辦潛在資料洩漏管道予以限制存取。

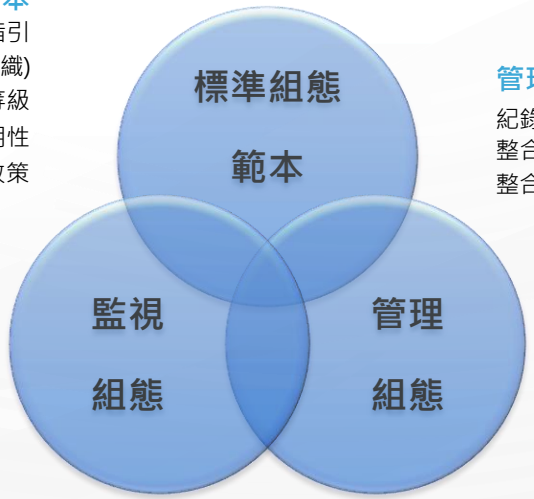
5. 作業內容

5.1 基於雲端服務協議通常係預先定義， 不可協商。對於所有雲端服務，本公司應審查與雲端服務提供者之雲端服務協議。雲端服務協議宜因應組織之機密性、完整性、可用性及資訊處理要求事項， 並具適切的雲端服

A.8.9 組態管理

編號	項目名稱	控制措施
8.9	組態管理	應建立、文件化、實作、監視和審查硬體、軟體、服務和網路的組態，包括安全組態。

標準組態範本
公開可用的指引
(例如：政府或安全組織)
考量所需保等級
考量組織環境適用性
考量組織資安政策



管理組態
紀錄組態資訊
整合資產管理流程
整合變更管理流程

監視組態
監視並定期審查
有誤差應採矯正措施

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
1	Windows 10 Account Settings	TWG CB-01-005-0001	帳戶原則\密碼原則	密碼最短使用期限	▪此項原則設定決定在使用者變更密碼之前，密碼必須使用的期限(天數)。可以設定 1 與 998 天之間的值，或設定天數為 0，以允許立即變更 ▪「密碼最短使用期限」不得超過「密碼最長使用期限」，除非「密碼最長使用	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼最短使用期限	1 天

項次	TWGCB-ID	類別	原則設定名稱	說明	D-Link 設定路徑	EDIMAX 設定路徑	ZyXEL 設定路徑
5	TWGCB-03-001-0005		變更預設 SSID	變更預設的 SSID，並且採用不足以識別為特定組織所使用之無線網路名稱	Basic Settings > Wireless Settings > Network Name (SSID) > Rename	Wireless Setting > Basic > SSID > Rename	Network > Wireless LAN 2.4G/5G > General > Network Name(SSID) > Rename
6	TWGCB-03-001-0006		關閉 SSID 廣播	▪關閉 SSID 的廣播模式，並要求使用者自行記錄連線的 SSID ▪這作法並不能避免有經驗的攻擊者發現 SSID，但仍應作為安全防護的一個部分	Basic Settings > Wireless Settings > SSID Visibility > Disable	Wireless Setting > Security > Broadcast SSID > Disable	Network > Wireless LAN 2.4G/5G > General > Hide SSID > Enable
7	TWGCB-03-001-0		降低無線網路設備	為防止攻擊者透過高功率天線進行無	Advanced Settings > Performance Settings	Wireless Settings > Advanced > Tx	Network > Wireless LAN 2.4G/5G >

A.8.10 資訊刪除

編號	項目名稱	控制措施
8.10	資訊刪除	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。

補充提醒：

- 所謂「刪除」係指「該資料/資訊無法被復原」。
- 須注意常被忽略的資訊：
  - 儲存於其他位置的過時版本、副本和暫時資訊。
  - 儲存於雲服務或外部廠商的資料返還與刪除。
  - 儲存於組織外儲存媒體的資訊 (遠距備份、遠距工作、行動裝置...等)。
  - 設備或媒體送修時的資料清理。

A.8.12 預防資料洩漏

編號	項目名稱	控制措施
8.12	預防資料洩漏	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。

識別和分級資訊

識別應防止洩漏之資訊，例如：個人資料、營業秘密...等。

監視與偵測資訊洩露管道

例如：電子郵件、文件傳輸、網路存取、行動設備和儲存設備...等。

採取措施防止資訊洩露

阻擋可能洩露敏感資訊的操作，例如：隔離包含敏感資訊的電子郵件、防止將資料庫資料複製到Excel文件...等。

A.8.28 安全程式設計

編號	項目名稱	控制措施
8.28	安全程式設計	軟體開發應採用安全編碼原則。

規劃及開發前 → 程式及開發期間 → 審查及維護

新開發或重新使用

安全政策、編碼原則、過往編碼缺陷、開發工具、人員訓練、安全開發環境..等。

開發期間或上線前

特定程式語言安全實作與編寫技術、結構化程式編寫、開發中測試..等。

程式碼上線後或修改

安全上版與部署、弱點處理、記錄錯誤與可疑攻擊、保護源碼、函式庫更新..等。

GAIA Information Technology

新版實作常見問題

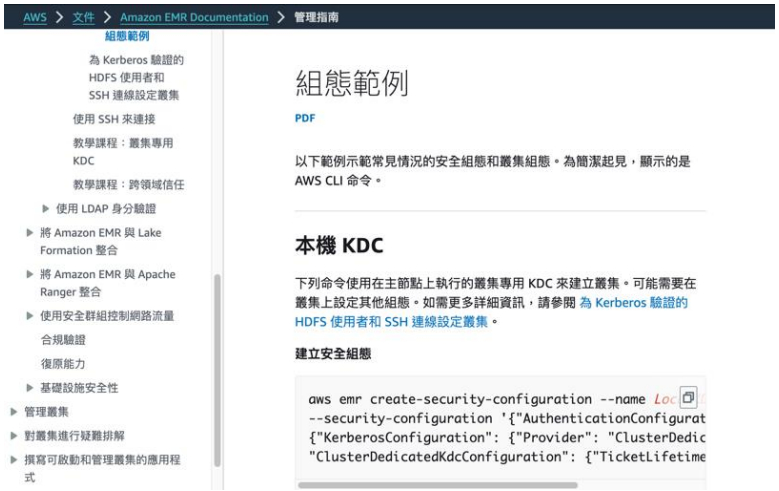
Q1:組態管理涵蓋範圍？

涵蓋四大主題：軟體、硬體、網路、服務

只要管理硬體的組態就好

A：涵蓋四大主題：軟體、硬體、網路、服務

編號	項目名稱	控制措施
8.9	組態管理	應建立、文件化、實作、監視和審查硬體、軟體、服務和網路的組態，包括安全組態。



參考資料： https://www.nics.nat.gov.tw/GCB.htm?lang=zh
https://docs.aws.amazon.com/zh_tw/emr/latest/ManagementGuide/

Q2: 雲端服務涵蓋範圍？

考慮ISMS範圍內
使用到的所有
雲端服務

僅考慮 IaaS
（基礎架構即服務）

A：ISMS範圍內使用到的所有雲服務

編號	項目名稱	控制措施
5.23	使用雲端服務之資訊安全	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。

- **現行雲端架構主要分成4類：自建雲、IaaS、PaaS、SaaS。**

- **IaaS（基礎設施即服務）：**
  是最基本的雲端運算服務，使用者可隨需存取**IT基礎架構服務**，包括：伺服器、儲存、網路及作業系統。
- **PaaS（平台即服務）：**
  提供雲端應用程式開發所需的軟硬體資源，透過PaaS，使用者可全心投入開發、測試、傳遞與管理軟體應用程式。
- **SaaS（軟體即服務）：**
  由**雲端供應商負責開發、維護、更新軟體**，使用者只要透過網際網路以訂閱方式購買軟體應用程式。

資料來源：蓋亞資訊 https://www.gaia.net/tc/news_detail/2/184

Q3:安全程式設計對於安全檢測的要求？

有做源碼檢測就可以

完整的檢測、檢測結果分析
判斷、弱點處理

A：完整的檢測、檢測結果分析判斷、弱點處理

編號	項目名稱	控制措施
8.29	開發及驗收中之安全測試	宜於開發生命週期中定義並實作安全測試過程。

- **新資訊系統、升級及新版本於開發期間完整測試及查證。**
- **安全測試為整體系統測試或組件測試一部分。**
- **擬訂測試計畫，包括下列事項：**
  - 活動及測試之**詳細排程**。
  - 於各項條件之範圍下之輸入及預期輸出。
  - 用以**評估結果之準則**。
  - 對必要時將採取之**進一步行動**的決策。

GAIA Information Technology

新版驗證時程

ISO 27001新版驗證服務時程

ISO 27001:2022建置/轉版輔導建議

現況分析	對於公司現有資安管理制度作業進行比對，檢視是否可符合新版要求
教育訓練	針對相關同仁進行教育訓練，確保可以完全瞭解新版標準之要求
管理文件建立/調整	建立/調整適用性聲明書，並依照差異分析結果，建立/調整現有管理文件
風險管理作業	依照更新後之管理制度，執行/調整風險管理作業
技術調整/升級	依據新版要求，確認現有技術管制作為是否可以符合。如無法符合，建立調整及升級計畫
管理制度運作調整	依照調整過後之管理文件及技術作業流程，調整資安管理制度運作及記錄

Thank You.

www.GAA.net

Google

官網請google搜尋...

蓋亞資訊

-歡迎關注蓋亞-