ISO 27001:2013 標準條文釋義
(資訊安全管理系統-要求)

資深顧問師 彭至賢 (Sam Peng)

ISO27001/BS10012/ISO9001主導稽核員

TPIPAS管理師&驗證師/PMP&APMP國際專案管理師

TTQS國家訓練品質計畫-評核委員

Mobile: 0952-695460

E-mail: sam@safelink.com.tw

SafeLink 博創資訊科技股份有限公司

ISO 27001:2013 標準條文

0. 簡介
1. 適用範圍
2. 引用標準
3. 用語釋義
4. 組織背景
5. 領導力
6. 計畫
7. 支援
8. 運作
9. 績效評估
10. 改進

0. 簡介

- 0.1 概述
- 0.2 與其他管理系統標準之相容性

0.1 概述 (1/2)

- **本標準乃是為了提供建立、實施、維護與持續改進一個資訊安全管理系統 (Information Security Management System, ISMS) 的要求而籌備的。**
- 組織的 ISMS 之設計與實施受其需求與目標、安全要求、所採用的過程以及組織之規模及架構所影響。這些要素的全部預期會隨時間而改變。
- ISMS 透過一個風險管理架構的適用，來保護資訊的機密性、完整性與可用性，且此資訊安全被列入充分管理的考量裡。
- ISMS 是組織過程和總體管理架構的一部分，且此資訊安全被列入過程的設計裡。**期望 ISMS 的實施與組**情況只需簡單的 ISMS 解決

並不是希望所有
導入ISO 27001的
機構制度都一樣

0.1 概述 (2/2)

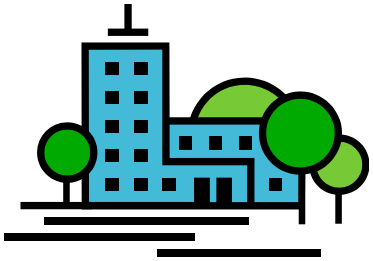
- 本標準適用於包含驗證機構的內部與外部團體，藉以評鑑組織達成自身資訊安全要求的能力。
- 在本標準裡呈現的要求之先後並非代表其重要性以及實施的順序。所列的項目僅供參考。
- ISO/IEC 27000 描述了 ISMS 的概述與詞彙，形成 ISMS 標準系列的主軸 (包含ISO/IEC 27003、ISO/IEC 27004和ISO/IEC 27005)，且定義出相關的用語釋義。

0.2 與其他管理系統標準之相容性

- 本標準適用了ISO/IEC Directives，Part 1 綜合 ISO 補充中的附錄 SL 所明定的高層次架構、相同的子條款標題、相同的文本、共通用語與核心定義，因而維持與其他已採用附錄 SL 的管理系統標準之相容性。
- 附錄 SL 所明定的共通作法，對於那些選擇運作可滿足兩種或多種管理系統標準的要求之單一管理系統，將是非常有用的。

1. 適用範圍

- 標準規定在組織背景內建立、實施、運作、維持及持續改進 ISMS 的要求。
- 本標準也包含了適合於組織需求的資訊安全風險評鑑與處理之要求。
- 本標準敘述之要求為一般性的，且適用所有組織，與其型式、規模大小或性質無關。在組織宣稱符合本標準時，排除本標準第 4 章至第 10 章所規定之任何要求，均不被接受。



2. 引用標準

- 下列參考文件，在整體或部分上，在本文件裡屬規範性的參考且對其應用是不可或缺的。
  - 有註記日期的引用標準，僅適用於引用的版本。
  - 未註記日期的引用標準，適用於該引用標準的最新版本 (包括任何修訂)。
- ISO/IEC 27000 資訊技術-安全技術-資訊安全管理系統-概述與詞彙。

3. 用語釋義

- 為本文件之目的，適用 ISO/IEC 27000 所明訂的用語釋義。

4. 組織背景

- 4.1 了解組織與其背景
- 4.2 了解利害相關團體的需求與期望
- 4.3 決定資訊安全管理系統的適用範圍
- 4.4 資訊安全管理系統

4.1 了解組織與其背景

- 組織應決定與其目的相關，且會影響其 ISMS 預期結果的達成能力之外部與內部問題。
- 備考：
  - 這些問題的決定，請參考 ISO 31000：2009 的條款 5.3 中建立組織外部與內部環境的考量事項。

4.2 了解利害相關團體的需求與期望

- a) 與ISMS 有關的利害相關團體；以及
- b) 與資訊安全有關的這些利害相關團體之要求。
- 備考：這些利害相關團體的要求可能包含了法規要求與契約義務。

4.3 決定資訊安全管理系統的適用範圍

- 組織應決定 ISMS 的界線與適用性，以建立其適用範圍。當決定適用範圍時，組織應考量：
  - a) 4.1 所提到的外部與內部問題；
  - b) 4.2 所提到的要求；以及
  - c) 在組織與其他組織執行的活動之間的接合與互賴關係。
- 此適用範圍應予以文件化資訊並易於取得。

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、維持和持續改進ISMS。

5. 領導力

- 5.1 領導力與承諾
- 5.2 政策
- 5.3 組織角色、責任與職權

5.1 領導力與承諾

- 高階管理者應展現領導力，以及與 ISMS 有關的承諾，藉由：
  - a) 確保資訊安全政策與目標已建立，並且和組織的策略方向是相容的；
  - b) 確保 ISMS 的要求已融入組織過程中；
  - c) 確保 ISMS 所需的資源可取得；
  - d) 傳達有效資訊安全管理的重要性，並且遵守 ISMS 的要求；
  - e) 確保 ISMS 達成其預期效果；
  - f) 指導與支援人員，使其對ISMS 的有效性做出貢獻；
  - g) 促進持續改進；以及
  - h) 支援其他的相關管理角色，讓其展現出在職責運用上之領導力。

5.2 政策

- 高階管理者應建立一個資訊安全政策，是：
  - a) 符合組織目的；
  - b) 包含資訊安全目標 (見6.2)，或提供訂立資訊安全目標的框架；
  - c) 包含對滿足有關資訊安全之適用要求的承諾；以及
  - d) 包含對 ISMS 持續改進的承諾。
- a) 資訊安全政策應：為文件化資訊並可取得；
- b) 在組織內流通；以及
- c) 適當時，利害相關團體可取得。

5.3 組織角色、責任與職權

- 高階管理者應確保有關資訊安全的角色之責任與職權已分配和傳達。
- 高階管理者應分配責任與職權，以：
  - a) 確保 ISMS 遵守本標準的要求；以及
  - b) 報告 ISMS 的績效給高階管理者。
- 備考：高階管理者也可分配責任與職權，在組織內可報告 ISMS 之績效。

6. 計畫

- 6.1 風險與機會的應對措施
- 6.2 資訊安全目標與實現的計畫

6.1 風險與機會的應對措施

- 6.1.1 概述
- 6.1.2 資訊安全風險評鑑
- 6.1.3 資訊安全風險處理

6.1.1 概述

- 當計劃 ISMS 時，組織應考量 4.1 所提到的問題與 4.2 所提到的要求，並且決定需要應對的風險與機會，以：
  - a) 確保 ISMS 可達成其預期結果；
  - b) 預防或減輕不良影響；以及
  - c) 達成持續改進。
- 組織應計劃：
  - a) 因應這些風險與機會的措施；以及
  - b) 如何
    - 1) 在其 ISMS 過程中融入並實施這些措施；以及
    - 2) 評估這些措施的有效性。

6.1.2 資訊安全風險評鑑

- 組織應明訂一個資訊安全風險評鑑的過程，可：
  - a) 建立與維持資訊安全風險的標準，包含了
    - 1) 可接受風險標準；以及
    - 2) 執行資訊安全風險評鑑的標準；
  - b) 確保重複的資訊安全風險評鑑能產出一致的、有效的和可比較的結果；
  - c) 識別資訊安全風險
    - 1) 適用的資訊安全評鑑過程，以識別與ISMS 範圍內之資訊機密性、完整性與可用性損害有關之風險；
    - 2) 識別風險負責人。
  - d) 分析資訊安全風險
    - 1) 評鑑會產生的潛在後果，如果在6.1.2 c) 1)識別的風險發生時；
    - 2) 評鑑在6.1.2 c) 1)識別的風險，其實際發生的可能性；
    - 3) 決定風險程度。
  - e) 評估資訊安全風險
    - 1) 比較被分析的風險與在6.1.2 a)建立的風險標準；及
    - 2) 把被分析的風險區分出風險處理的優先順序。
  - 組織應保存有關資訊安全風險評鑑過程的文件化資訊。

6.1.3 資訊安全風險處理

- 組織應明訂與適用一個資訊安全處理過程，以：
  - a) 選擇適當的資訊安全風險處理之選項，將風險評鑑結果列入考量；
  - b) 決定在實施選用的資訊安全處理選項時，必需的所有管制項；
    - 備考：組織可依據需要設計管制，或從任何來源識別它們。
  - c) 比較在上述6.1.3 b)決定的管制與附錄A 的，且確認沒有忽略到必要的管制；
    - 備考 1：附錄A包含了一個有關管制目標與管制的詳細清單。本標準的使用者參考附錄A，以確保沒有忽略到重要的管制選項。
    - 備考 2：管制目標已隱含在選用的管制中。列在附錄A的管制目標與管制不夠詳盡，所以可能需要額外的管制目標與管制。
  - d) 創作一個適用性的聲明，要包含必需的管制(見6.1.3 b) 與 c)，以及無論是否進行實施，包含之的正當理由，還有附錄A的管制排除之正當理由；
  - e) 制定一個資訊安全風險處理計畫；
  - f) 獲得風險負責人對資訊安全風險處理計畫的核准，以及接受殘留的資訊安全風險。
  - 組織應保存資訊安全風險處理過程的文件化資訊。
  - 備考：本標準的資訊安全風險評鑑與處理過程和 ISO 31000 所提供的原則與通用指南是相互配合的。

6.2 資訊安全目標與實現的計畫

- 組織應在相關的職能與層級上，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。
- 組織應保存資訊安全目標的文件化資訊。
- 當計劃如何達成其資訊安全目標時，組織應決定：
  - f) 要做什麼；
  - g) 需要什麼資源；
  - h) 誰要負責；
  - i) 何時完成；且
  - j) 如何評估結果。

7. 支援

- 7.1 資源
- 7.2 人員能力
- 7.3 認知
- 7.4 溝通
- 7.5 文件化資訊

7.1 資源

- 組織應決定與提供用來建立、實施、維持和持續改進 ISMS 所需的資源。

7.2 人員能力

- 組織應：
  - a) 決定會影響資訊安全績效，受其管制的工作人員所必需的能力；
  - b) 確保這些人員能勝任，以適當的教育、訓練或經驗為根據；
  - c) 適用時，採取措施以取得必需的能力，且評估採取的措施之有效性；以及
  - d) 保存適當的文件化資訊當作能力的證據。
  - 備考：適用的措施可能包含，舉例來說，對目前員工提供訓練、監督或調動；或是僱用有能力的人員或與其締約。

7.3 認知

- 受組織管制的工作人員應認知到：
  - a) 資訊安全政策；
  - b) 對 ISMS 有效性之貢獻，包含了改進資訊安全績效之好處；以及
  - c) 不符合ISMS 要求的含義。

7.4 溝通

- 組織應決定與 ISMS 有關的內部與外部溝通之需求，包含了：
  - a) 要溝通什麼；
  - b) 何時溝通；
  - c) 和誰溝通；
  - d) 應是誰溝通；以及
  - e) 應實現哪種溝通過程。

7.5 文件化資訊

- 7.5.1 概述
- 7.5.2 創造與更新
- 7.5.3 文件化資訊的管制

7.5.1 概述

- 組織的 ISMS 應包含：
  - a) 本標準必需的文件化資訊；以及
  - b) 由組織決定，ISMS 的有效性所必需的文件化資訊。
  - 備考：一個 ISMS 的文件化資訊之廣度會在不同組織間有所差異，因為：
    - 1) 組織的規模，以及其活動、過程、產品與服務的類型；
    - 2) 過程的複雜性與相互作用；以及
    - 3) 人員的能力。

7.5.2 創造與更新

- 當創造與更新文件化資訊時，組織應確保適當的：
  - a) 識別與描述 (例如一個標題、日期、作者、或參考編號)；
  - b) 格式 (例如語言、軟體版本、圖表) 與媒介 (例如紙本、電子)；以及
  - c) 適用性與充足性的審查和核准。

7.5.3 文件化資訊的管制

- ISMS 與本標準必需的文件化資訊應受管制以確保：
  - a) 在需要的地點與時間，可取得且適當使用；
  - b) 受到充分的維護 (例如避免機密性的損害、使用不當、或完整性的損害)；
- 對於文件化資訊的管制，適用時，組織應應對下列的活動：
  - c) 分配、存取、修復、使用；
  - d) 貯藏與保存，包含保存易讀性；
  - e) 變更管制 (例如版本的變更)；以及
  - f) 保留與廢除。
- 由組織決定，ISMS 的計畫與運作所必需的外部來源之文件化資訊，適當時應識別之且接受管制。
- 備考：存取意指著一個決定，關乎文件化資訊僅作借閱的許可、或是文件化資訊借閱和變更的許可與職權等等。

8. 運作

- 8.1 運作的計畫與管制
- 8.2 資訊安全風險評鑑
- 8.3 資訊安全風險處理

8.1 運作的計畫與管制

- 組織應計畫、實施與管制可符合資訊安全要求，及實施在 6.1 決定的措施時所需要的過程。組織也應實施計畫，以達成在 6.2 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。
- 組織應確保外包過程是確定的並受管制。

8.2 資訊安全風險評鑑

- 組織應在計劃之期間內，或是當重大的變更被提出或發生時，執行資訊安全風險評鑑，並考量在 6.1.2 a) 建立的標準。
- 組織應保存資訊安全風險評鑑結果的文件化資訊。

8.3 資訊安全風險處理

- 組織應實施資訊安全風險處理的計畫。
- 組織應保存資訊安全風險處理結果的文件化資訊。

9. 績效評估

- 9.1 監督、量測、分析與評估
- 9.2 內部稽核
- 9.3 管理階層審查

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。
  - a) 什麼需要監督與量測，包含資訊安全過程與管制；
  - b) 監督、量測、分析與評估的方法，適用時，用以確保有效的結果；
    - 備考：選用的方法得產生可比較與可重現的結果，才能認定為有效。
  - c) 監督與量測應何時執行；
  - d) 應由誰監督與量測；
  - e) 從監督與量測得來的結果應何時分析與評估；以及
  - f) 應由誰分析與評估這些結果。
- 組織應保存適當的文件化資訊，作為監督與量測結果的證據。

9.2 內部稽核

- 組織應在計劃之期間內執行內部稽核，以提供資訊，指出 ISMS 是否：
  - a) 符合
    - 1) 組織本身有關 ISMS 的要求；以及
    - 2) 本標準的要求；
  - b) 有效地實施與維護。
- 組織應：
  - c) 計畫、建立、實施與維護一個稽核流程，包含了頻率、方法、責任、計畫中的要求與報告。稽核流程應考量相關過程的重要性，以及先前稽核的結果；
  - d) 為每一場稽核明訂稽核標準與適用範圍；
  - e) 選擇稽核員並執行稽核，以確保稽核過程的客觀與公正；
  - f) 確保稽核結果已向相關管理者報告；以及
  - g) 保存文件化資訊，作為稽核流程與稽核結果的證據。

9.3 管理階層審查

- 高階管理者應在時間間隔內審查組織的 ISMS，以確保其持續的適用性、充足性與有效性。
- 管理審查應包含的考量事項：
  - a) 先前管理審查的措施之狀態
  - b) 有關 ISMS 的外部與內部問題之變更；
  - c) 資訊安全的績效回饋，包含下列趨向：
    - 1) 不符合事項與矯正措施；
    - 2) 監督與量測結果；
    - 3) 稽核結果；以及
    - 4) 資訊安全目標的實現；
  - d) 利害相關團體的回饋；
  - e) 風險評鑑的結果與風險處理計畫的狀態；以及
  - f) 持續改進的機會；
- 管理審查的產出應包含和持續改進機會與 ISMS 的變更需求有關之決定。
- 組織應保存文件化資訊，管理審查結果的證據。

10. 改進

- 10.1 不符合事項與矯正措施
- 10.2 持續改進

10.1 不符合事項與矯正措施

- 當一個不符合事項發生，組織應：
  - a) 適用時，對不符合事項作出回應：
    - 1) 採取措施管制與矯正之；以及
    - 2) 處理後果；
  - b) 評估消除不符合事項的原因之措施需求，為了使其不再發生或是在別處發生，經由：
    - 1) 審查不符合事項；
    - 2) 決定不符合事項的原因；以及
    - 3) 決定是否有相似的不符合事項存在，或有發生的潛在性；
  - c) 實施任何需要的措施；
  - d) 審查任何採取的矯正措施之有效性；以及
  - e) 必要時，對 ISMS 作變更；
- 矯正措施應適用於所遇到的不符合事項之影響。
- 組織應保存文件化資訊，作為下列證據：
  - f) 不符合事項的本質與任何採取的後續措施；以及
  - g) 任何矯正措施的結果。

10.2 持續改進

- 組織應持續改進 ISMS 的適切性、充份性與有效性。

附錄A. 參考的控制目標與控制措施

- A.5 資訊安全政策
- A.6 資訊安全的組織
- A.7 人力資源安全
- A.8 資產管理
- A.9 存取控制
- A.10 密碼
- A.11 實體與環境安全
- A.12 作業的安全
- A.13 通訊安全
- A.14 資訊系統獲取、開發及維護
- A.15 供應商關係
- A.16 資訊安全事故管理
- A.17 營運持續管理的資訊安全層面
- A.18 遵循性

ISO 27001:2013 控制措施 → A.5

- A.5 資訊安全政策
  - A.5.1 資訊安全的管理方向
    - 目標：依照營運需要及相關法律與法規，提供管理階層對資訊安全之指示與支持。

ISMS *Information Security Management System*

ISO 27001:2013 控制措施 → A.5.1

- A.5.1 資訊安全的管理方向
  - A.5.1.2 資訊安全政策
    - 控制措施：資訊安全的一系列政策應明訂出來、受管理階層核准、發布並傳達給員工與相關的外部團體。
  - A.5.1.2 資訊安全政策之審查
    - 控制措施：資訊安全政策應依計畫之期間或發生重大變更時審查，以確保其持續的適用性、充分性與有效性。

ISO 27001:2013 控制措施 → A.6

- A.6 資訊安全的組織
  - A.6.1 內部組織
    - 目標：建立一個管理框架，用以開創與管制組織內資訊安全的實施和操作。
  - A.6.2 行動設備與遠距工作
    - 目標：確保遠距工作與使用行動設備的安全

ISO 27001:2013 控制措施 → A.6.1

- A.6.1 內部組織
  - A.6.1.1 資訊安全的角色與責任
    - 控制措施：所有的資訊安全責任應予明訂與分配
  - A.6.1.2 職務的區隔
    - 控制措施：相互衝突的職務與責任領域應加以區隔，以降低組織資產遭未經授權或非故意的修改或誤用之機會。
  - A.6.1.3 與權責機關的聯繫
    - 控制措施：應與相關權責機關維持適當聯繫
  - A.6.1.4 與特殊利害相關團體的聯繫
    - 控制措施：應與各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.6.1.5 專案管理的資訊安全
    - 控制措施：不論何種類型的專案管理都應依循資訊安全

ISO 27001:2013 控制措施 → A.6.2

- A.6.2 行動設備與遠距工作
  - A.6.2.1 行動設備的政策
    - 控制措施：應採取適當政策與輔助的安全措施，以管理使用行動設備所導致的風險。
  - A.6.2.2 遠距工作
    - 控制措施：應落實政策與輔助的安全措施，以保護在遠距工作所存取、處理或儲存的資訊。

ISO 27001:2013 控制措施 → A.7

- A.7 人力資源安全
  - A.7.1 聘僱之前
    - 目標：確保員工與承包商了解他們的責任，且適合他們被認定的角色。
  - A.7.2 聘僱期間
    - 目標：確保員工與承包商認知並履行其資訊安全的責任
  - A.7.3 聘僱的終止與變更
    - 目標：保護組織的利益，作為變更或終止聘僱的過程之一部分。

ISO 27001:2013 控制措施 → A.7.1

- A.7.1 聘僱之前
  - A.7.1.1 篩選
    - 控制措施：應依照相關法律、法規及倫理，並兼顧營運要求的相稱性、所存取資訊的保密類別及所察覺的風險，對所有聘僱之應徵者的背景予以查核。
  - A.7.1.2 聘僱條款與條件
    - 控制措施：與員工和承包商的契約協議應陳述其與組織對資訊安全的責任

ISO 27001:2013 控制措施 → A.7.2

- A.7.2 聘僱期間
  - A.7.2.1 管理階層責任
    - 控制措施：管理階層應要求員工及承包商，依照組織既定的政策與程序實施資訊安全事宜。
  - A.7.2.2 資訊安全認知、教育及訓練
    - 控制措施：組織所有員工和相關的承包商，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知教育及訓練。
  - A.7.2.3 懲處過程
    - 控制措施：對違反資訊安全的員工所採取的措施，應有一個正式且經過溝通之懲處過程。

ISO 27001:2013 控制措施 → A.7.3

- A.7.3 聘僱的終止與變更
  - A.7.3.1 聘僱責任的終止與變更
    - 控制措施：在聘僱的終止或變更生效、傳達予員工或承包商並強制執行之後，資訊安全的責任與義務仍然有效。

ISO 27001:2013 控制措施 → A.8

- A.8 資產管理
  - A.8.1 資產責任
    - 目標：鑑別組織的資產與明訂適當的保護責任
  - A.8.2 資訊分類
    - 目標：確保資訊受到適切等級的保護，依照其對組織的重要性。
  - A.8.3 媒體的處置
    - 目標：防止儲存在媒體的資訊被未經授權的揭露、修改、移除或破壞。

ISO 27001:2013 控制措施 → A.8.1

- A.8.1 資產責任
  - A.8.1.1 資產清冊
    - 控制措施：應識別與資訊和資訊處理設施相關的資產，且應制訂與維持這些資產的清冊。
  - A.8.1.2 資產的擁有權
    - 控制措施：清冊內所維持的資產管理權應被指派
  - A.8.1.3 資產之可被接受的使用
    - 控制措施：與資訊處理設施相關的資訊與資產，其可被接受的使用之規則應予以識別、文件化及實施。
  - A.8.1.4 資產歸還
    - 控制措施：所有的員工與外部團體使用者，在其聘僱、契約或協定終止後應立即歸還全部的組織資產。

ISO 27001:2013 控制措施 → A.8.2

- A.8.2 資訊分類
  - A.8.2.1 資訊分類
    - 控制措施：資訊應依法規要求、價值、危害性與對未經授權的揭露或修改之敏感性觀點予以分類。
  - A.8.2.2 資訊標示
    - 控制措施：應依照組織所採用的分類法，發展與實施一套適當的資訊標示程序。
  - A.8.2.3 資產處置
    - 控制措施：應依照組織所採用的分類法，發展與實施資產處置程序。

ISO 27001:2013 控制措施 → A.8.3

- A.8.3 媒體的處置
  - A.8.3.1 可攜式媒體的管理
    - 控制措施：應依照組織所採用的分類法，實施可攜式媒體管理之程序。
  - A.8.3.2 媒體的處理
    - 控制措施：媒體不再需要時，應使用正式程序加以安全地汰除。
  - A.8.3.3 實體媒體的傳送
    - 控制措施：應保護含有資訊的媒體在傳送期間，不受未經授權的存取、誤用或毀損。

ISO 27001:2013 控制措施 → A.9

- A.9 存取控制
  - A.9.1 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.9.2 使用者存取管理
    - 目標：確保經授權使用者對系統與服務的存取及防止未經授權的存取
  - A.9.3 使用者責任
    - 目標：讓使用者在維護他們的鑑別資訊上負責
  - A.9.4 系統與應用系統的存取控制
    - 目標：防止對系統與應用系統的未授權存取

ISO 27001:2013 控制措施 → A.9.1

- A.9.1 存取控制的營運要求
  - A.9.1.1 存取控制政策
    - 控制措施：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 網路與網路服務的存取
    - 控制措施：應僅提供使用者經特定授權可存取使用的網路與網路服務

ISO 27001:2013 控制措施 → A.9.2

- A.9.2 使用者存取管理
  - A.9.2.1 使用者登錄與註銷
    - 控制措施：應實施一個正式的使用者登錄與註銷登錄程序，以使所指派的存取權限可行。
  - A.9.2.2 使用者的存取配置
    - 控制措施：應實施一個正式的使用者存取權限配置程序，以對所有系統與服務的全部使用者類型分配和撤銷存取權限。
  - A.9.2.3 特權的管理
    - 控制措施：應限制與控制特權存取權限的配置與使用
  - A.9.2.4 使用者的機密授權資訊之管理
    - 控制措施：機密授權資訊的配置，應透過一個正式的管理過程加以控制。
  - A.9.2.5 使用者存取權限的審查
    - 控制措施：資產所有人應定期審查使用者的存取權限
  - A.9.2.6 存取權限的移除或調整
    - 控制措施：所有的員工與外部團體使用者對資訊與資訊處理設施的存取權限，在其聘僱、契約或協定的終止後應移除之，或是在變更後作調整。

ISO 27001:2013 控制措施 → A.9.3

- A.9.3 使用者責任
  - A.9.3.1 機密授權資訊的使用
    - 控制措施：在機密授權資訊的使用，使用者必須遵循組織的安全作法。

ISO 27001:2013 控制措施 → A.9.4

- A.9.4 系統與應用系統的存取控制
  - A.9.4.1 資訊存取限制
    - 控制措施：應根據存取控制政策，限制資訊與應用系統功能的存取。
  - A.9.4.2 安全之登入程序
    - 控制措施：在存取控制政策的要求下，應由安全的登入程序控制系統與應用系統的存取。
  - A.9.4.3 通行碼管理系統
    - 控制措施：通行碼管理系統應為互動式，並應確保通行碼之嚴謹。
  - A.9.4.4 特權的公用程式之使用
    - 控制措施：應限制與嚴密控制可能篡改系統與應用控制措施的公用程式之使用
  - A.9.4.5 程式源碼的存取控制
    - 控制措施：應限制對程式源碼的存取

ISO 27001:2013 控制措施 → A.10

- A.10 密碼
  - A.10.1 密碼控制措施
    - 目標：確保密碼的適當與有效使用，以保護資訊的機密性、鑑別性與/或完整性。

ISO 27001:2013 控制措施 → A.10.1

- A.10.1 密碼控制措施
  - A.10.1.1 使用密碼控制措施的政策
    - 控制措施：使用密碼控制措施以保護資訊的政策應加以發展與實施
  - A.10.1.2 金鑰管理
    - 控制措施：有關密碼金鑰的使用、保護與期限之政策應通過整個運用週期加以發展與實施。

ISO 27001:2013 控制措施 → A.11

- A.11 實體與環境安全
  - A.11.1 安全區域
    - 目標：防止組織的資訊與資訊處理設施遭未經授權的存取、損害及干擾。
  - A.11.2 設備
    - 目標：防止資產的遺失、損害、竊盜或破解，並防止組織運作的中斷。

ISO 27001:2013 控制措施 → A.11.1

- A.11.1 安全區域
  - A.11.1.1 實體安全邊界
    - 控制措施：應界定與使用安全邊界，藉以防護敏感的或是重要的資訊與資訊處理設施之區域。
  - A.11.1.2 實體進出管制
    - 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 實施辦公場所及設施之安全管制
    - 控制措施：應規劃並實施辦公室、房間及設施的實體安全
  - A.11.1.4 對外部與環境威脅的保護
    - 控制措施：應規劃並實施實體保護，以避免遭受自然災害、惡意攻擊或意外。
  - A.11.1.5 在安全區域內工作
    - 控制措施：應規劃並實施在安全區域內工作的程序
  - A.11.1.6 收發與裝卸區
    - 控制措施：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出入口應加以控制，並盡可能與資訊處理設施隔離，以避免未經授權的存取。

ISO 27001:2013 控制措施 → A.11.2

- A.11.2 設備 (1/2)
  - A.11.2.1 設備安置與保護
    - 控制措施：應安置或保護設備，以降低來自環境之威脅與危機造成的風險，以及未經授權存取之機會。
  - A.11.2.2 支援的設施
    - 控制措施：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的中斷
  - A.11.2.3 佈纜的安全
    - 控制措施：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 設備維護
    - 控制措施：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 資產的攜出
    - 控制措施：未經事前授權，設備、資訊或軟體不應帶出場外。

ISO 27001:2013 控制措施 → A.11.2

- A.11.2 設備 (2/2)
  - A.11.2.6 駐外設備的安全
    - 控制措施：安全措施應適用於駐外資產，並應考量其在組織場所外工作的各種不同風險。
  - A.11.2.7 設備的汰除或再使用之安全
    - 控制措施：含有儲存媒體的設備，其所有項目在汰除或再使用前應加以驗證，以確保任何敏感性的資料與授權軟體已被移除或安全地覆寫。
  - A.11.2.8 無人看管的用戶設備
    - 控制措施：使用者應確保無人看管的設備有適當保護
  - A.11.2.9 桌面淨空與螢幕淨空政策
    - 控制措施：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。

ISO 27001:2013 控制措施 → A.12

- A.12 作業的安全
  - A.12.1 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.12.2 防範惡意程式
    - 目標：確保資訊與資訊處理設施對惡意程式的防範
  - A.12.3 備份
    - 目標：防範資料的損失
  - A.12.4 存錄與監控
    - 目標：紀錄事件與生成證據
  - A.12.5 作業軟體的控制
    - 目標：確保作業系統的完整性
  - A.12.6 技術脆弱性管理
    - 目標：防範技術脆弱性的利用
  - A.12.7 資訊系統稽核考量
    - 目標：使作業系統上的稽核活動之衝擊降至最低

ISO 27001:2013 控制措施 → A.12.1

- A.12.1 作業之程序與責任
  - A.12.1.1 文件化作業程序
    - 控制措施：操作程序應加以文件化，並讓有需要的所有使用者均可隨時取得。
  - A.12.1.2 變更管理
    - 控制措施：對會影響資訊安全之組織、營運過程及資訊處理設施與系統的變更應予控制。
  - A.12.1.3 容量管理
    - 控制措施：應監視、調諧(tune)各項資源的使用，並對未來容量要求預作規劃，以確保所要求的系統績效。
  - A.12.1.4 開發、測試及運作環境的分隔
    - 控制措施：應分隔開發、測試及運作之環境，以降低對運作環境未經授權存取或變更的風險。

ISO 27001:2013 控制措施 → A.12.2

- A.12.2 防範惡意程式
  - A.12.2.1 對抗惡意程式的控制措施
    - 控制措施：偵測、預防及復原控制以防範惡意程式的機制及結合適切的使用者認知程序應被施行。

ISO 27001:2013 控制措施 → A.12.3

- A.12.3 備份
  - A.12.3.1 資訊備份
    - 控制措施：應依照備份政策，定期進行資訊、軟體及系統的備份與測試。

ISO 27001:2013 控制措施 → A.12.4

- A.12.4 存錄與監控
  - A.12.4.1 事件存錄
    - 控制措施：事件日誌係紀錄使用者活動、異常、錯誤及資訊安全事件，應產生、保留並定期審查。
  - A.12.4.2 日誌資訊的保護
    - 控制措施：應保護存錄設施與日誌資訊，不受竄改與未經授權的存取。
  - A.12.4.3 管理者與操作者日誌
    - 控制措施：系統管理者與操作者的活動應加以存錄、保護並定期審查。
  - A.12.4.4 時脈同步
    - 控制措施：組織或安全網域內所有相關資訊處理系統的時脈，應與單一的參考時間來源同步。

ISO 27001:2013 控制措施 → A.12.5

- A.12.5 作業軟體的控制
  - A.12.5.1 作業系統上軟體的安裝
    - 控制措施：應實施程序，以控制作業系統上軟體的安裝。

ISO 27001:2013 控制措施 → A.12.6

- A.12.6 技術脆弱性管理
  - A.12.6.1 技術脆弱性的管理
    - 控制措施：應及時取得關於使用中資訊系統之技術脆弱性的資訊，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的風險。
  - A.12.6.2 軟體安裝的限制
    - 控制措施：應建立與實施管理使用者之軟體安裝的規則。

ISO 27001:2013 控制措施 → A.12.7

- A.12.7 資訊系統稽核考量
  - A.12.7.1 資訊系統稽核控制
    - 控制措施：有關作業系統的驗證，應謹慎規劃及議定其稽核要求與活動，使營運過程之中斷降至最低。

ISO 27001:2013 控制措施 → A.13

- A.13 通訊安全
  - A.13.1 網路安全管理
    - 目標：確保對網路內資訊與支援性資訊處理設施的保護
  - A.13.2 資訊轉換
    - 目標：維護組織內及與外部個體所轉換資訊的安全

ISO 27001:2013 控制措施 → A.13.1

- A.13.1 網路安全管理
  - A.13.1.1 網路控制措施
    - 控制措施：網路應加以管理與控制，以保護系統與應用系統的資訊。
  - A.13.1.2 網路服務的安全
    - 控制措施：應識別所有網路服務的安全機制、服務水準及管理要求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 網路區隔
    - 控制措施：應將資訊服務、使用者及資訊系統各群組使用的網路加以區隔。

ISO 27001:2013 控制措施 → A.13.2

- A.13.2 資訊轉換
  - A.13.2.1 資訊轉換政策與程序
    - 控制措施：應備妥正式的轉換政策、程序及控制措施，以保護經由各種形式通訊設施的資訊轉換。
  - A.13.2.2 資訊轉換的協議
    - 控制措施：應有因應組織與外部團體間之營運資訊安全轉換之協議
  - A.13.2.3 電子傳訊
    - 控制措施：電子傳訊涉及的資訊應適當地加以保護
  - A.13.2.4 機密性或不揭露協議
    - 控制措施：相對組織於資訊保護需要之機密性或不揭露協議要求，應加以識別、定期審查並予文件化。

ISO 27001:2013 控制措施 → A.14

- A.14 資訊系統獲取、開發及維護
  - A.14.1 資訊系統的安全要求
    - 目標：確保跨越整個生命週期內，資訊安全是整體資訊系統的一部份。這也包含在提供有關公共網路服務之資訊系統的要求中。
  - A.14.2 開發與支援過程的安全
    - 目標：確保資訊安全被整合至資訊系統開發生命週期之設計與實施之中。
  - A.14.3 測試資料
    - 目標：確保測試用途之資料的保護

ISO 27001:2013 控制措施 → A.14.1

- A.14.1 資訊系統的安全要求
  - A.14.1.1 資訊安全要求分析與規格
    - 控制措施：在新資訊系統或現有系統的提升，應納入資訊安全相關的要求
  - A.14.1.2 公共網路應用系統之安全服務
    - 控制措施：涉及通過公共網路應用系統服務之相關資訊，應防範詐騙活動、合約爭議及未授權揭漏與修改。
  - A.14.1.3 保護應用系統服務之交易
    - 控制措施：涉及應用系統服務之交易的資訊應加以保護，以防範不完整傳輸、錯誤路由、未授權的訊息改變、披露、複製或重現。

ISO 27001:2013 控制措施 → A.14.2

- A.14.2 開發與支援過程的安全 (1/2)
  - A.14.2.1 安全開發政策
    - 控制措施：應建立軟體與系統的開發規則，並適用於組織內的開發。
  - A.14.2.2 系統變更控制程序
    - 控制措施：應藉由使用正式的變更控制程序，以控制開發過程中的系統變更
  - A.14.2.3 作業平台變更後的應用系統技術審查
    - 控制措施：作業平台變更時，應審查與測試關鍵應用系統，以確保對組織作業或安全無不利的衝擊。
  - A.14.2.4 套裝軟體變更的限制
    - 控制措施：應避免軟體套件之修改，且僅限於有必要的變更，並應嚴格管制所有的變更。

ISO 27001:2013 控制措施 → A.14.2

- A.14.2 開發與支援過程的安全 (2/2)
  - A.14.2.5 安全系統工程原則
    - 控制措施：應建立安全系統工程的原則並予維護及文件化，且適用於任何資訊系統的實施工作。
  - A.14.2.6 安全開發環境
    - 控制措施：組織應對涵蓋整個系統的開發與整合工作，建立安全開發環境並予適當地保護。
  - A.14.2.7 委外開發
    - 控制措施：組織應監督與監視委外系統開發的活動
  - A.14.2.8 系統安全測試
    - 控制措施：安全功能的測試應在開發期間進行
  - A.14.2.9 系統驗收測試
    - 控制措施：應建立新資訊系統、升級及新版本的驗收測試流程與相關標準。

ISO 27001:2013 控制措施 → A.14.3

- A.14.3 測試資料
  - A.14.3.1 測試資料的保護
    - 控制措施：應慎選、保護及管制測試資料。

ISO 27001:2013 控制措施 → A.15

- A.15 供應商關係
  - A.15.1 供應商關係的資訊安全
    - 目標：確保供應商可存取之組織資產的保護
  - A.15.2 供應商服務交付管理
    - 目標：維持議定等級之資訊安全及服務交付，並能與供應商協議一致。

ISO 27001:2013 控制措施 → A.15.1

- A.15.1 供應商關係的資訊安全
  - A.15.1.1 供應商關係的資訊安全政策
    - 控制措施：應與供應商協議資訊安全要求，以減少供應商對組織資產存取的風險並加以文件化。
  - A.15.1.2 供應商協議內的安全處理
    - 控制措施：應建立所有相關的資訊安全要求，並與每項可存取、處理、儲存、傳達組織資訊或提供IT基礎設施組件的供應商達成協議。
  - A.15.1.3 ICT 供應鏈
    - 控制措施：與供應商的協議，應包含因應有關資訊與通訊技術服務及產品供應鏈之資訊安全風險的要求。

ISO 27001:2013 控制措施 → A.15.2

- A.15.2 供應商服務交付管理
  - A.15.2.1 供應商服務的監控與審查
    - 控制措施：組織應定期監控、審查及稽核供應商提供之服務。
  - A.15.2.2 供應商服務變更的管理
    - 控制措施：供應商所提供服務的變更，包含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及風險重新評鑑。

ISO 27001:2013 控制措施 → A.16

- A.16 資訊安全事故管理
  - A.16.1 資訊安全事故與改進的管理
    - 目標：確保資訊安全事故管理之一致與有效的作法，包含安全事件與弱點的傳達。

ISO 27001:2013 控制措施 → A.16.1

- A.16.1 資訊安全事故與改進的管理 (1/2)
  - A.16.1.1 責任與程序
    - 控制措施：應建立管理責任與程序，以確保對資訊安全事故做迅速、有效及依序的回應。
  - A.16.1.2 通報資訊安全事件
    - 控制措施：應循適切的管理管道，儘速通報資訊安全事件。
  - A.16.1.3 通報資訊安全弱點
    - 控制措施：應要求使用組織資訊系統與服務有關的員工與承包商，注意並通報系統或服務之任何觀察到或可疑的資訊安全弱點。

ISO 27001:2013 控制措施 → A.16.1

- A.16.1 資訊安全事故與改進的管理 (2/2)
  - A.16.1.4 資訊安全事件的評鑑與決定
    - 控制措施：應評鑑資訊安全事件，並決定是否歸類為資訊安全事故。
  - A.16.1.5 對資訊安全事故的回應
    - 控制措施：應依據文件化程序對資訊安全事故作回應
  - A.16.1.6 從資訊安全事故中學習
    - 控制措施：藉分析與解決資訊安全事故獲得的知識應用，以降低未來事故的可能性或衝擊。
  - A.16.1.7 證據的收集
    - 控制措施：組織應對可作為證據之資訊，明定適用的識別、收集、獲取及保存程序。

ISO 27001:2013 控制措施 → A.17

- A.17 營運持續管理的資訊安全層面
  - A.17.1 資訊安全的持續性
    - 目標：資訊安全持續應嵌入組織的營運持續管理裡
  - A.17.2 複式配置
    - 目標：確保資訊處理設施的可用性

ISO 27001:2013 控制措施 → A.17.1

- A.17.1 資訊安全的持續性
  - A.17.1.1 規劃資訊安全的持續性
    - 控制措施：組織應決定在不利情況下，例如：一場危機或災難期間，其資訊安全與資訊安全管理系統持續性之要求。
  - A.17.1.2 實施資訊安全持續
    - 控制措施：組織應建立、文件化、實施及維持過程、程序及控制措施，以確保在不利情況期間，維持資訊安全的必要等級。
  - A.17.1.3 驗證、審查及評估資訊安全持續
    - 控制措施：組織應定期驗證已建立及實施的資訊安全持續之控制措施，以確保在不利情況時，它們是適切且有效的。

ISO 27001:2013 控制措施 → A.17.2

- A.17.2 複式配置
  - A.17.2.1 資訊處理設施的可用性
    - 控制措施：資訊處理設施應有足夠的複式配置，以符合可用性要求。

ISO 27001:2013 控制措施 → A.18

- A.18 遵循性
  - A.18.1 遵循適法性與契約要求
    - 目標：避免違反有關資訊安全的法律、法令、法規或契約義務，以及任何安全要求。
  - A.18.2 資訊安全審查
    - 目標：確保資訊安全是依據組織政策與程序實施與操作。

ISO 27001:2013 控制措施 → A.18.1

- A.18.1 遵循適法性與契約要求
  - A.18.1.1 識別適用之法規與契約要求
    - 控制措施：對每一個資訊系統與組織，所有相關法律法規、規章與契約要求及組織用以符合此等要求之方法，宜加以明確界定、文件化及維持最新。
  - A.18.1.2 智慧財產權
    - 控制措施：應實施適當程序，以確保有關智慧財產權與所使用的專屬軟體產品，可遵循法律、法規及契約的要求。
  - A.18.1.3 紀錄的保護
    - 控制措施：應依據法律、法規、契約及營運要求，保護紀錄免於遺失、毀損、偽造、未授權的存取與發佈。
  - A.18.1.4 隱私權與個人識別資訊的之保護
    - 控制措施：應遵循相關的適用法令與法規所要求，確保隱私權及個人識別資訊的保護。
  - A.18.1.5 密碼控制措施的規定
    - 控制措施：應使用密碼控制措施，以遵循所有相關的協議、法律及法規。

ISO 27001:2013 控制措施 → A.18.2

- A.18.2 資訊安全審查
  - A.18.2.1 資訊安全的獨立審查
    - 控制措施：應在計畫的間隔內或當發生重大變更時，獨立審查組織資訊安全的管理與實施作法(例如資訊安全的控制目標、控制措施、政策、過程及程序)。
  - A.18.2.2 安全政策與標準的遵循性
    - 控制措施：管理人員應藉由適當的安全政策、標準及任何其他安全要求，定期審查資訊處理的遵循性與其責任範圍內的程序。
  - A.18.2.3 技術遵循性檢查
    - 控制措施：應定期審查資訊系統是否遵循組織的資訊安全政策與標準。

Q&A 問題與討論

～如有任何問題，歡迎隨時來電詢問～

SafeLink

博創資訊科技股份有限公司

臺中市南屯區大墩三街159-1號

TEL：886-4-24719945

FAX：886-4-24712948

http://www.safelink.com.tw/

E-mail: sam@safelink.com.tw