財團法人國家實驗研究院
國家地震工程研究中心

『資訊安全管理制度維護案』

教育訓練

資安法令宣導及ISO27001標準介紹課程(一)

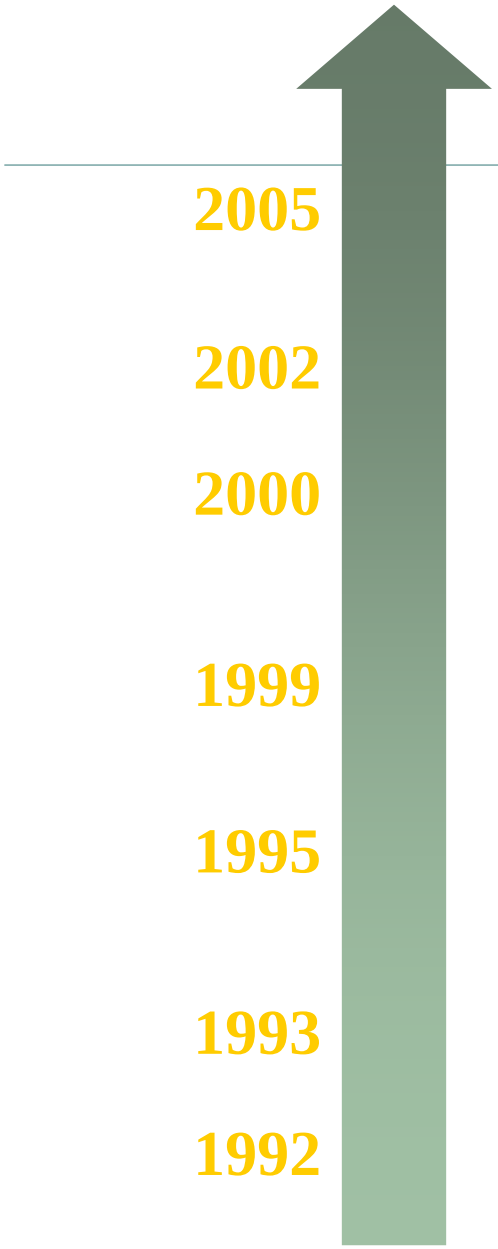
98年06月09日(二)

講師：邱瑩青

財團法人中華民國國家資訊基本建設產業發展協進會

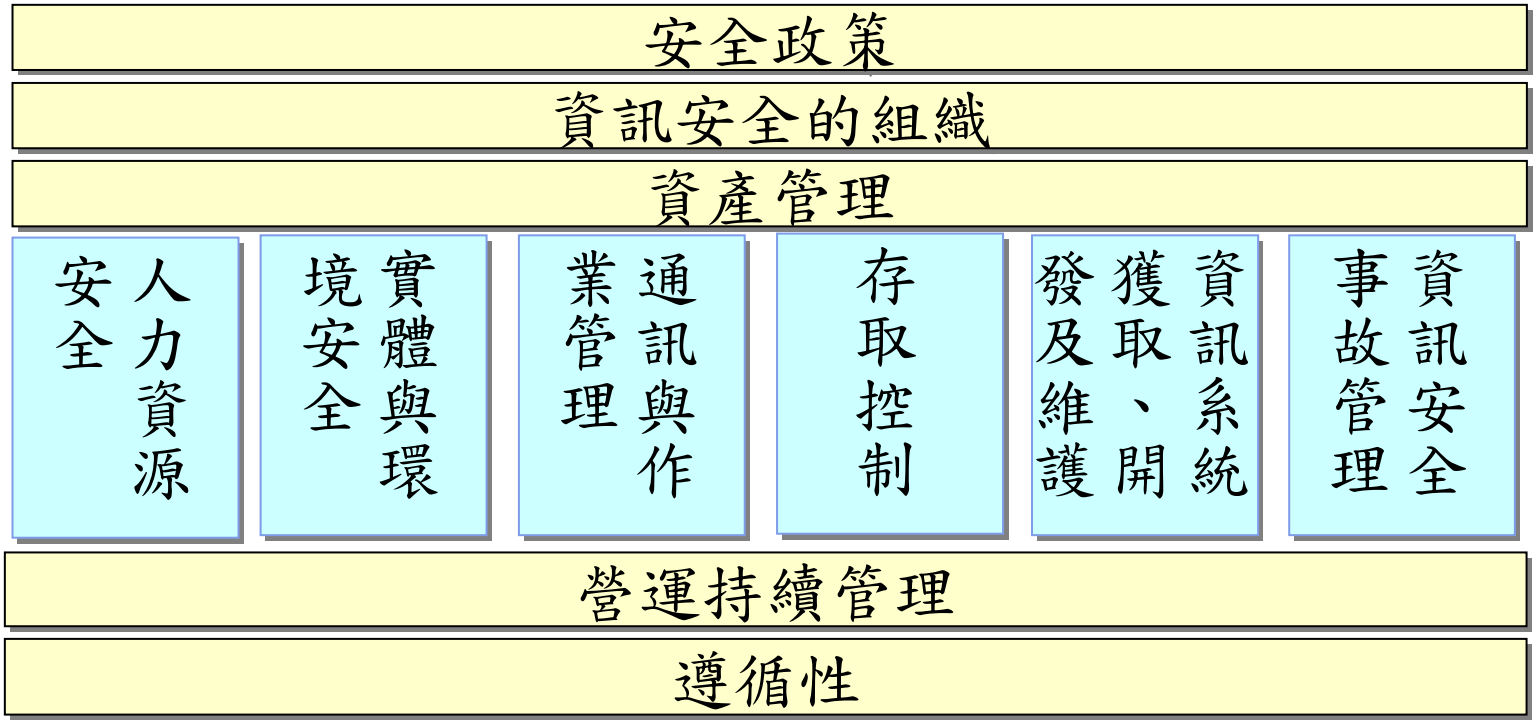
ISO/CNS 27001:2005
標準說明

財團法人中華民國國家資訊基本建設產業發展協進會



2005	發行ISO 27001:2005 改版ISO 17799:2005
2002	9月正式公佈BS 7799-2: 2002
2000	12月正式成為ISO 17799標準 提交ISO組織討論(ISO DIS 17799)
1999	新版英國標準 BS 7799 Part 1 & 2發行
1995	英國公佈BS 7799 Part 2 英國公佈BS 7799 Part 1
1993	率先由英國貿易工業部進行專案
1992	世界經濟開發組織(OECD);資訊系統安全指導方針

11 個領域、 39 個控制目標、 133 個控制措施



目錄

簡介

財團法人中華民國國家資訊基本建設產業發展協進會

0.1 概說

- 建立、實施、操作、監督、審查、維持及改進資訊安全管理系統。
- 組織的策略性決策。
- 影響設計與執行因素：
  - 組織需求
  - 目標
  - 安全要求
  - 組織作業程序
  - 組織規模與架構
- 若狀況簡單就只需要簡單的資訊安全管理系統方案。
- 適用於有利害相關之內部與外部團體。

0.2過程導向Process approach

- 採用過程導向(作法)，鼓勵其使用者強調下列事項之重要性：

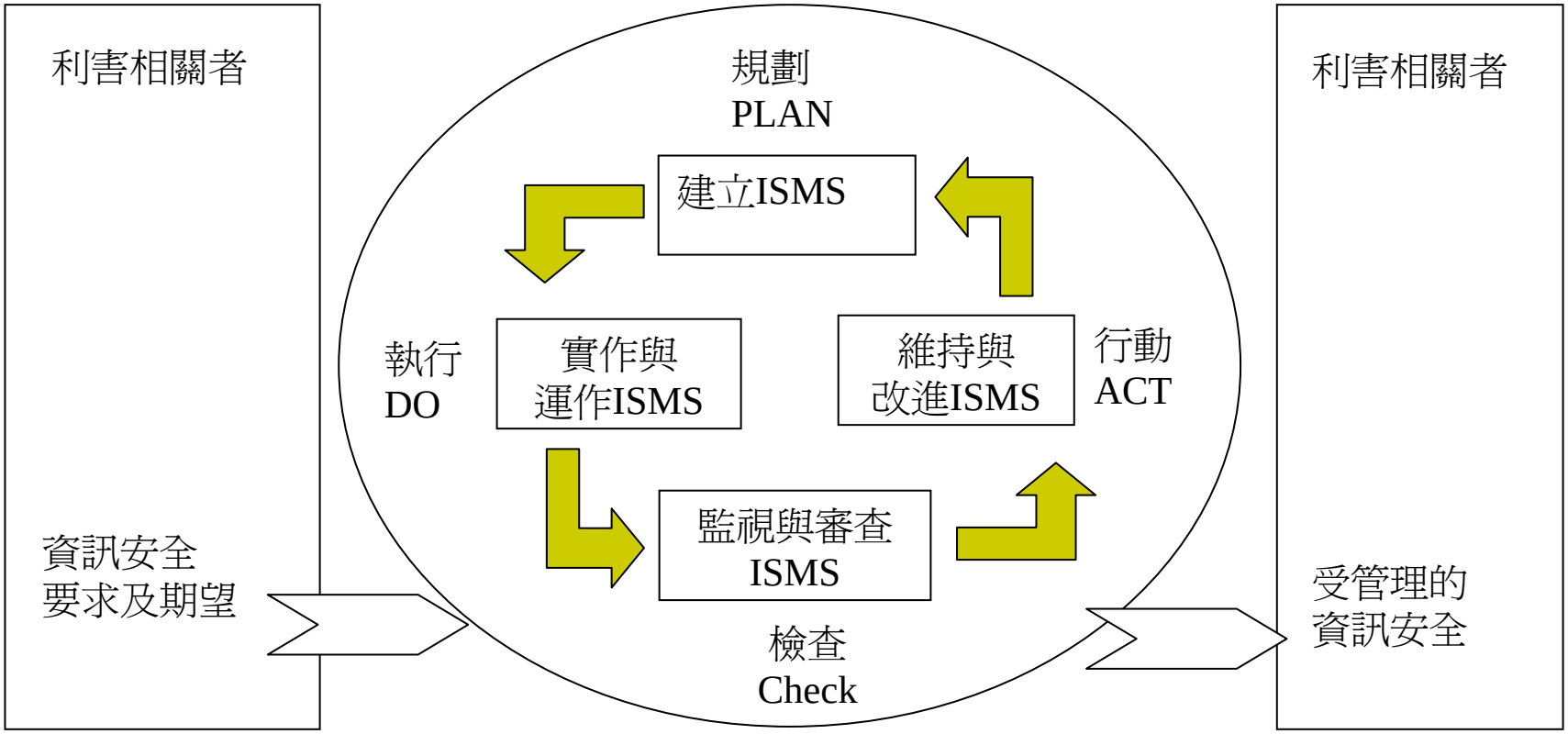
(a) 瞭解組織資訊安全要求，以及瞭解建立資訊安全之政策與目標的需求。

(b) 在組織整體營運風險之全景(context) 中，實作及運作各項控制措施以管理組織的資訊安全風險。

(c) 監視與審查ISMS 之績效與有效性。

(d) 基於客觀的測量以持續改進。

ISMS過程的PDCA模型



1 適用範圍

1.1 概論

- 涵蓋所有類型的組織。
- 規範建立、實施、操作、監督、審查、維持及改進一份包含組織整體營運風險之文件化資訊安全管理系統之要求。
- 確保選擇適切的及相稱的安全控制措施，以保護資訊資產並提供利害相關者信心。

1.2應用

- 敘述之要求為一般性的，且適用所有組織，與其類型、規模大小及業務性質無關。
- 排除本標準第4 節至第8 節所規定之任何要求，均不被接受 。
- 排除任何控制措施時，除非不影響該由風險評鑑及適用之法規要求所決定之安全要求的資訊安全之能力及/或責任，均不被接受。

2引用標準

- ISO/IEC 17799:2005 (CNS 17799:2005)

3 術語和定義

3.1資產asset

對組織有價值的任何事物。

3.2 可用性availability

獲得授權的實體要求時可以存取並使用的特性。

3.3 機密性confidentiality

資訊不被未經授權的個人、實體或過程取得或揭露的特性。

3.4 資訊安全information security

保護資訊的機密性、完整性與可用性；另外也能涉及如鑑別性、 可歸責任性、 不可否認性與可靠性等特性。

3.5 資訊安全事件information security event

系統、服務或網路狀態經鑑別而顯示示可能有違反資訊安全政策或保護措施失效，或可能與安全有關但事先未知狀況的發生。

3.6資訊安全事故information security incident

單一或一連串有顯著機率可能危害營運作業與威脅資訊安全，而不希望發生或非預期的資訊安全事件。

3.7資訊安全管理系統

information security management system ISMS

整體管理系統的一部份，以營運風險方案為基礎，用以建立、實施、操作、監督、審查、維持及改進資訊安全。

3.8完整性 integrity

保護資產準確及完整的特性。

3.9 剩餘風險residual risk

經過風險處理後剩餘的風險。

3.10風險接受(risk acceptance)

決定接受某風險。

3.11風險分析(risk analysis)

系統性的使用資訊，以識別緣由與估計風險。

3.12風險評鑑(risk assessment)

風險分析與風險評估的整個過程。

3.13風險評估(risk evaluation)

把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。

3.14風險管理(risk management)

藉由協調各項活動以指導與控管組織之有關風險。

3.15風險處理(risk treatment)

選擇與實作措施的過程藉以修正風險。

3.16適用性聲明(statement of applicability)

描述與組織之ISMS 相關且對其適用之各項控制目標與控制措施的已文件化聲明。

4 資訊安全管理系統

財團法人中華民國國家資訊基本建設產業發展協進會

4.1一般要求

- 組織應在其整體營運活動與其所面臨風險的全景中，建立、實作、運作、監視、審查、維持及改進已文件化之ISMS 。
- 採用之過程以PDCA 模型為基礎。

4.2建立與管理ISMS

4.2.1 建立ISMS

(a)依據營運、組織、其所在位置、資產及技術等特性，並納入該範圍內所有排除項目的細節和衡量理由，來界定ISMS 之範圍及諸邊界。

4.2.1 建立ISMS(續)

(b)依據營運、組織、其所在位置、資產及技術等特性，界定ISMS 政策：

(1) 設定目標之框架，整體意識及各項行動原則。

(2)考量營運與法律或法規要求，以及契約的安全義務。

(3)與組織的策略性風險管理全景相校準，ISMS 在此全景中建立及維持。

(4)建立可藉以評估風險之準則。

(5)由管理階層所核准。

4.2.1 建立ISMS(續)

(c)界定組織的風險評鑑作法。

(1)識別適合ISMS 及已識別之營運資訊安全、法律與法規要求的風險評鑑方法論。

(2)發展風險接受的準則，並識別風險可接受的等級。所選擇的風險評鑑方法應確保風險評鑑產生可比較與可再產生的結果。

4.2.1 建立ISMS(續)

(d)識別各項風險。

(1)識別ISMS 範圍內之各項資產以及此等資產之擁有者。

(2)識別對該等資產的各項威脅。

(3)識別此等威脅可能利用之各項脆弱性。

(4)識別對此等資產可能造成機密性、完整性及可用性之損失的各項衝擊。

4.2.1 建立ISMS(續)

(e)分析與評估各項風險。

(1)評鑑安全失效時可能造成對組織之營運衝擊，並將資產的機密性、完整性及可用性之損失的後果納入考量。

(2)根據最常見之威脅、脆弱性(弱點)及與此等資產有關的衝擊，以及現行實作的控制措施，來評鑑此種安全失效發生的實際可能性。

(3)估計各風險之等級。

(4)決定風險是否可接受或使用建立之風險接受準則來處理。

4.2.1 建立ISMS(續)

(f)識別並評估風險處理之各項選項作法。

(1)採用適切的控制措施。

(2)若其明顯的符合組織的政策與風險接受準則，則知悉與客觀地接受此等風險。

(3)迴避風險。

(4)轉移相關之營運風險至他者。

4.2.1 建立ISMS(續)

(g)選擇各項風險之處理的控制目標與控制措施。

應選擇並實作控制目標與控制措施，以符合由風險評鑑和風險處理過程所識別的各項要求。此選擇應考量風險接受準則， 以及法律、法規與契約的要求。

4.2.1 建立ISMS(續)

(h)取得管理階層對所提議之各項剩餘風險的核准。

(i)取得管理階層對實作和運作ISMS 的授權

(j)擬定一份適用性聲明書，內容包括。

(1) 選擇之各項控制目標與控制措施，以及其選擇之理由。

(2)目前已實作的各項控制目標與控制措施。

(3)所排除之所有附錄A 中之各項控制目標與控制措施及其被排除的衡量理由。

4.2.2 實作與運作ISMS

(a) 架構一項風險處理計畫，以識別適當管理措施、資源、責任及優先順序。

(b)實作風險處理計畫，達成各項控制目標，計畫中包括資金的考量以及角色與責任的配置。

(c)實作所選擇的控制措施，以符合控制目標。

(d)界定量測控制措施或控制措施群有效性的措施，並規定如何使用量測措施，以產生可比較與可再產生的結果。

4.2.2 實作與運作ISMS(續)

(e)實作訓練與認知計畫。

(f)管理ISMS 的運作。

(g)管理ISMS 的資源。

(h)實作能立即偵測安全事件與回應安全事故之程序以及其他各項控制措施。

4.2.3 監視與審查ISMS

(a)執行監視與審查程序以及其他控制措施，以便：

(1)立即的偵測出處理結果之錯誤。

(2)立即的識別試圖的與已成功的安全危害和事故。

(3)使管理階層能判定實作的各項安全活動，是否如預期般履行。

(4)使用各項指標，以協助偵測安全事件，並預防安全事故。

(5)判定所採取解決安全危害的措施是否有效。

(b)定期審查ISMS 的有效性(包括是否符合ISMS 政策與目標，以及安全控制措施的審查)，並將安全稽核、事故、有效性測量，以及來自所有利害相關者之建議與回饋之結果納入考量。

(c)量測控制措施的有效性，以查證已符合各項安全要求。

4.2.3 監視與審查ISMS(續)

(d)定期審查風險評鑑，並審查剩餘風險的等級與已識別的可接受風險，並考量下列變更：

(1)組織。

(2)技術。

(3)各項營運目標與過程。

(4)已識別的威脅。

(5)已實作之控制措施的有效性。

(6)外部事件。

(e)依已規劃的期間施行ISMS 內部稽核。

(f)定期執行ISMS 之管理階層審查，以確保維持適當範圍，及ISMS 過程之各項改進。

(g)考量監視與審查活動的發現，以更新安全計畫。

(h)記錄對ISMS 有效性或績效有衝擊之措施與事件。

4.2.4 維持與改進ISMS

(a)實作所識別之ISMS 各項改進。

(b) 採取適當矯正與預防措施。並運用從其他組織及由組織本身之安全經驗中習得之教訓。

(c) 與所有利害相關者就各項措施與改進進行溝通，並協議進行方式。

(d)確保各項改進達到其預期目標。

4.3文件化要求

4.3.1 概述

文件化應：

- 確保各項措施可追溯至管理階層決策及政策。
- 確保所記錄的結果是可再產生的。
- 展示選擇的控制措施和風險評鑑與風險處理過程的結果間之關係，
- 展示選擇的控制措施和ISMS 政策與目標間之關係。

4.3.1 概述(續)

ISMS 文件化應包括：

(a) ISMS 政策與各項目標之已文件化聲明。

(b) ISMS 之範圍。

(c) 支援ISMS 之各項程序及控制措施。

(d) 風險評鑑方法論的描述。

(e) 風險評鑑報告。

(e)風險處理計畫。

(f)組織為確保有效規劃、運作及控制其資訊安全過程，以及描述如何量測控制措施的有效性所需之文件化程序。

(g)標準要求之各項紀錄。

(h)適用性聲明書。

4.3.2 文件管制

(a) 在文件發行前核准其適切性。

(b) 必要時，審查與更新並重新核准文件。

(c) 確保文件之變更與最新修訂狀況已予以識別。

(d) 確保在使用處，備妥適切版本之適用文件。

(e) 確保文件保持易於閱讀並容易識別。

(f) 確保文件對其需要者可隨時取得，且依據適用其分類的程序予以傳送、儲存以及最終作廢。

(g) 確保外部來源之文件已加以識別。

(h) 確保文件分發受管制。

(i) 防止作廢的文件被誤用。

(j) 作廢的文件若為任何目的而保留時，應施予適當識別。

4.3.3 紀錄管制

- 應建立並維持各項紀錄，以提供要求之符合性及ISMS之有效運作的證據。
- 紀錄應加以保護與管制。
- 應將任何相關的法律或法規要求以及契約義務納入考量。
- 紀錄應保持易於閱讀，容易識別及檢索。
- 文件化並實作紀錄之識別、儲存、保護、檢索、保存期限及作廢所需的各項控制措施。
- 應保存各項過程績效的紀錄，及所有重大安全事故發生之紀錄。

5 管理階層責任

財團法人中華民國國家資訊基本建設產業發展協進會

5.1管理階層承諾

- 管理階層應提供其對ISMS 之建立、實作、運作、監視、審查、維持與改進之承諾的證據：
  (a) 建立一份ISMS 政策。
  (b) 確保建立ISMS 各項目標及計畫。
  (c) 建立資訊安全之各種角色與責任。
  (d) 向組織傳達符合各項資訊安全目標、符合資訊安全政策及法律規範下之組織責任，以及持續改進之需求等的重要性。
  (e) 提供充分資源以建立、實作、運作、監視、審查、維持與改進ISMS。
  (f) 決定接受風險的準則與可接受風險等級的準則。
  (g) 確保施行內部ISMS 稽核。
  (h) 施行ISMS 之管理階層審查。

5.2資源管理

5.2.1 資源提供

提供下列工作所需資源：

(a) 建立、實作、運作、監視、審查、維持及改進ISMS 。

(b) 確保各項資訊安全程序支援營運要求。

(c) 識別並因應法律與法規要求，及契約的安全義務。

(d) 正確應用所有已實作的控制措施，以維護適當之安全。

(e) 必要時進行審查，並針對審查之結果作適切反應。

(e) 需要時，改進ISMS 之有效性。

5.2.2 訓練、認知及能力

(a) 決定履行影響ISMS 之工作的人員之必要能力。

(b) 提供訓練或採取其他措施(如聘僱有能力之人員)，以滿足此等需求。

(c) 評估所採措施之有效性。

(d) 維持教育、訓練、技能、經驗及評定資格等之紀錄。

(e) 組織亦應確保所有相關人員已認知其所從事的資訊安全活動之關聯性與重要性，以及他們如何對ISMS 各項目標之達成有所貢獻。

6 ISMS 內部稽核

財團法人中華民國國家資訊基本建設產業發展協進會

- 組織應依已規劃的期間施行ISMS 內部稽核，以判定其ISMS 之控制目標、控制措施、過程及程序是否：
  (a) 符合本標準及相關法律或法規的要求。
  (b) 符合所識別的資訊安全要求。
  (c) 被有效的實作與維持。
  (d) 如預期的履行。
- 稽核計畫應被規劃，並將過程與將受稽核的領域之狀況和重要性，以及先前稽核的結果納入考量。
- 稽核準則、範圍、頻率及方法應被界定。
- 稽核人員的選擇與稽核的施行應確保稽核過程的客觀性及公平性。
- 稽核人員不應稽核其本身的工作。規劃與施行稽核，以及報告結果與維持紀錄之責任與要求，應以文件化程序加以界定。
- 受稽核領域之負責管理階層，應確保所採行的措施無不當延誤，以致偵測出之不符合事項及其原因消失。
- 跟催活動應包括所採行措施之查證與查證結果之報告。

7 ISMS 之管理階層審查

財團法人中華民國國家資訊基本建設產業發展協進會

7.1 概述

- 管理階層應依已規劃的期間(至少一年一次)，審查組織的ISMS ，以確保其持續的適用性、適切性及有效性。
- 此項審查應包括評鑑改進之機會與評鑑ISMS變更之需求，包括資訊安全政策與資訊安全目標。
- 審查結果應清楚的文件化

7.2 審查輸入

(a) ISMS 稽核與審查之結果。

(b) 來自利害相關者之回饋。

(c) 可用於組織以改進ISMS 績效與有效性之技術、產品或程序。

(d) 預防與矯正措施之狀況。

(e) 於先前風險評鑑未適切因應之脆弱性或威脅。

(f) 有效性測量的結果。

(g) 先前管理階層審查之跟催措施。

(h) 可能影響ISMS 之任何變更。

(i) 改進之各項建議。

7.3 審查輸出

(a) ISMS 有效性之改進。

(b) 風險評鑑與風險處理計畫之更新。

(c) 影響資訊安全之程序與控制措施之必要時的修改，以回應可能衝擊ISMS 之內部或外部事件，包括下列事項之變更：

(1)各項營運要求。

(2)各項安全要求。

(3)影響既有各項營運要求之營運過程。

(4)法律或法規各項要求。

(5)契約的各項義務。

(6)風險等級及/或風險接受準則。

(d) 資源需求。

(e) 控制措施的有效性如何量測之改進。

8 ISMS 之改進

財團法人中華民國國家資訊基本建設產業發展協進會

8.1 持續改進

- 組織應藉由使用資訊安全政策、資訊安全目標、稽核結果、監視事件之分析、矯正與預防措施以及管理階層審查，以持續改進ISMS之有效性。

8.2 矯正措施

矯正措施應界定：

(a) 識別各項不符合事項。

(b) 判定各項不符合之原因。

(c) 評估措施之需求，以確保各項不符合事項不復發。

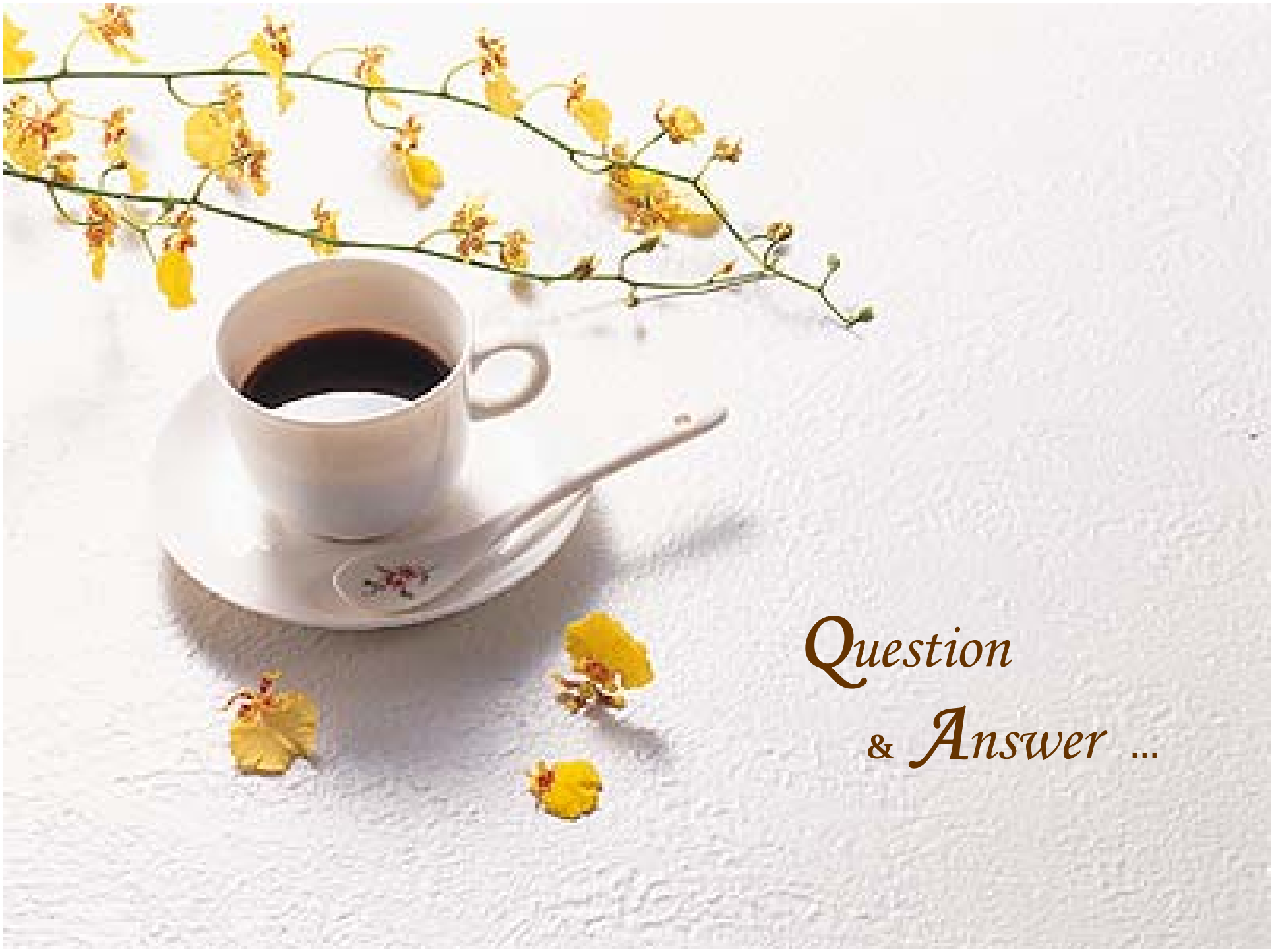
(d) 決定及實作所需之矯正措施。

(e) 記錄所採取措施的結果。

(f) 審查所採取之矯正措施。

8.3 預防措施

- 應決定措施，以消除與ISMS 要求潛在不符合之原因，並防止其發生。
- 預防措施應與潛在問題之衝擊相稱。
- 預防措施應界定：
  - (a) 識別潛在的各項不符合事項及其原因。
  - (b) 評估措施的需求，以防止不符合事項的發生。
  - (c) 決定及實作所需之預防措施。
  - (d) 記錄所採取措施之結果。
  - (e) 審查所採取之預防措施。
- 組織應識別已變更之風險並識別針對注意重大已變更之風險的預防措施之要求。
- 預防措施之優先順序，應依據風險評鑑之結果決定。


Question
& Answer ...