資訊安全管理系統
ISO 27001:
Specification for Information Security Management Systems

ISO 27001 內容

0. 簡介
1. 適用範圍
2. 引用標準
3. 術語與定義
4. 資訊安全管理系統
5. 管理責任
6. ISMS內部稽核
7. ISMS之管理階層審查
8. ISMS之改進

Annex A.控制措施和目的 (Controls and Objectives)
Annex B. OECD 原則與本標準
Annex C. BS EN ISO9001：2000, ISO14001：1996和本標準之間的對應關係
參考資料

1. 適用範圍 (Scope)

1.1 概論 (General)

- 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
- 設計乃爲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(application)

- 本國際標準敘述之要求爲一般性的，且適用所有組織，與其類型、規模大小及業務性質無關

2. 引用標準(Normative reference)

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

3. 術語和定義 (Terms and definitions)

3.1 資產(asset)

3.2 可用性(availability)

3.3 機密性(confidentiality)

3.4 資訊安全(information security)

3.5 資訊安全事件(information security event)

3.6 資訊安全事故(information security incident)

3.7 資訊安全管理系統(information security management system, ISMS)

3.8 完整性 (integrity)

3. 術語和定義(續)
(Terms and definitions)

3.9 殘餘風險(residual risk)

3.10 風險承受(risk acceptance)

3.11 風險分析(risk analysis)

3.12 風險評鑑(risk assessment)

3.13 風險評估(risk evaluation)

3.14 風險管理(risk management)

3.15 風險處理(risk treatment)

3.16 適用性聲明(statement of applicability)

4. 資訊安全管理系統 (Information security management system)

4.1 一般要求(General Requirements)

4.2 資訊安全管理系統建立與管理
(Establishing and managing the ISMS)

4.3文件化要求
(Documentation requirements)

4.2 資訊安全管理系統建立與管理 (Establishing and managing the ISMS)

4.2.1 建立資訊安全管理系統(Establish the ISMS)

4.2.2 實施與操作資訊安全管理系統 (Implement and operate the ISMS)

4.2.3 監控和審查資訊安全管理系統(Monitor and review the ISMS)

4.2.4 維持與改進資訊安全管理系統(Maintain and improve the ISMS)

。

4.2.1 建立資訊安全管理系統與管理(1) (Establishing the ISMS)

組織應執行下列事項 ：

a) 依據營運、組織、其所在位置、資產、技術等特性，以及包括任何該範圍所排除的細節和理由，界定資訊安全管理系統之範圍及界限

b) 依據營運、組織、其所在位置、資產及技術等特性，界定資訊安全管理系統之政策，且 ：

   1) 包括設定目標之框架，並建立與資訊安全有關之整體方向意識與行動原則；
   2) 考慮營運與法律或法規要求，以及合約的安全責任 ；
   3) 與組織的策略性風險管理內容相結合，使資訊安全管理系統得以建立及維護；
   4) 建立藉以評估風險的準則[參閱4.2.1 c節)]；
   5) 由管理階層所核准。

4.2.1 建立資訊安全管理系統與管理(2) (Establishing the ISMS)

c) 定義組織的風險評鑑方法
   1) 鑑別一風險評鑑方法，且可適合其資訊安全管理系統及已鑑別之營運資訊安全、法律與法規要求。
   2) 發展可承受風險的準則與鑑別可接受風險的程度。所選擇的風險評鑑方法應確保風險評鑑可產生可比較的與可再產生（reproducible）的結果。
d) 鑑別風險
   1) 鑑別在資訊安全管理系統範圍內的資產和資產的擁有者；
   2) 鑑別這些資產所受到的威脅；
   3) 鑑別可能被這些威脅利用的脆弱性；
   4) 鑑別對資產失去機密性、完整性和可用性的衝擊。

4.2.1 建立資訊安全管理系統與管理(3) (Establishing the ISMS)

e) 分析與評估風險
   1) 評鑑安全失效時可能對組織營運之衝擊，並將資產喪失機密性、完整性及可用性之後果列入考慮；
   2) 根據與這些資產有關之威脅、脆弱性及衝擊，以及現行所實施的控制措施，評鑑安全失效實際發生的可能性；
   3) 估計風險的等級；
   4) 決定風險是否可接受或要求使用第4.2.1c)2)節所建立之風險承受準則來處理。

4.2.1 建立資訊安全管理系統與管理(4) (Establishing the ISMS)

f) 鑑別並評估風險處理之選項作法

可能的作法包括：

1) 採用適當的控制措施；
2) 若提供風險明顯的符合組織的政策與風險承受準則(參閱第4.2.1c)，則可在掌握狀況下客觀的接受此等風險；
3) 迴避風險；
4) 將相關之營運風險轉移至其他機構，如：保險公司，供應商。

g) 選擇控制目標及控制措施以處理風險。

應選擇Annex A所列之各項控制目標與控制措施，作爲恰當涵蓋所鑑別各項要求之過程的一部份。

4.2.1 建立資訊安全管理系統與管理(5) (Establishing the ISMS)

h) 取得管理階層對所提議殘餘風險的核准。

i) 取得管理階層對實施和操作資訊安全管理系統的授權。

j) 擬定一份適用性聲明書。

適用性聲明書應準備包含下列事項：

1) 在4.2.1 g)中被選擇的控制目標和控制措施及選擇的理由；
2) 目前已經實施的控制目標和控制措施；
3) 附錄 A 中任何排除的控制目標和控制措施其排除的理由；

4.2.2 實施與操作資訊安全管理系統(1) (Implement and operate the ISMS)

組織應執行下列事項 ：

a) 架構一項風險處理計畫以鑑別適當管理措施、資源、職責及優先順序，以便管理資訊安全風險(參閱第5節)；

b) 實施風險處理計畫，以達到所鑑別的控制目標，計畫內容包括資金的考慮以及角色與職責的分派；

c) 實施第4.2.1 g)節所選擇的控制措施，以符合控制目標；

4.2.2 實施與操作資訊安全管理系統(2) (Implement and operate the ISMS)

d) 界定如何量測所選擇控制措施或控制措施群組的有效性，並規定如何使用這些量測去評核控制措施的有效性，以產生可比較與可再產生的結果(參閱第4.2.3c) 節)；

e) 實施訓練與認知的計畫（參閱第5.2.2節）；

f) 管理資訊安全管理系統的作業；

g) 管理資訊安全管理系統之資源（參閱第5節）；

h) 實施能立即偵測安全事件與回應安全事故之程序以及其他控制措施(參閱第4.2.3 節)。

4.2.3 監控和審查資訊安全管理系統(1) (Monitor and review the ISMS)

組織應執行下列事項 ：

a) 執行監督與審查程序，以及其他控制措施，以便：

1) 立即偵測處理結果之錯誤；
2) 立即鑑別有意圖的與成功的安全危害和事故；
3) 促使管理階層決定是否所委任的人員或藉由資訊技術所實施的各項安全活動，均已如預期般實行；
4) 藉由使用各項指標，以協助偵測安全事件，並預防安全事故；
5) 決定所採取的措施是否有效解決安全危害。

4.2.3 監控和審查資訊安全管理系統(2) (Monitor and review the ISMS)

b) 定期審查資訊安全管理系統的有效性(包含符合資訊安全管理系統政策與目標，以及安全控制措施的審查)，並考慮安全稽核的結果、事故、來自有效性量測的結果、以及來自所有利害相關者之建議與回饋。

c) 量測控制措施的有效性，以查證各項安全要求皆已符合。

4.2.3 監控和審查資訊安全管理系統(3) (Monitor and review the ISMS)

d) 在規劃的期間審查風險評鑑，並審查殘餘風險與已鑑別可接受風險的等級，並考慮下列之變化：
   1) 組織；
   2) 技術；
   3) 業務目標和過程；
   4) 已識別的威脅；
   5) 已實施控制措施的有效性；
   6) 外部事件，如法律或法規環境的變化、合約責任的變化、和社會環境的變化。

4.2.3 監控和審查資訊安全管理系統(4) (Monitor and review the ISMS)

e) 在已規劃的期間對於資訊安全管理系統進行內部稽核。

f) 定期執行資訊安全管理系統之管理階層審查，以確保其範圍維持適當，且資訊安全管理系統過程之各項改進均已鑑別(參閱第7.1節)。

g) 考量監督與審查活動的發現以更新安全計畫。

h) 記錄對資訊安全管理系統有效性或表現有衝擊的措施與事件（參閱第4.3.3節）。

4.2.4 維持與改進資訊安全管理系統 (Maintain and improve the ISMS)

組織應定期執行下列事項 ：

a) 實施資訊安全管理系統所鑑別之改進活動。
b) 依據第8.2及8.3節採取適當矯正與預防措施。採用從其他組織及組織本身之安全經驗吸取教訓。
c) 以適切於情況的詳盡程度，與所有利害相關者就各項措施與改進進行溝通，適當時並協議如何進行。
d) 確保各項改進措施達到其預期目標

4.3文件化要求 (Documentation requirements)

4.3.1 一般要求(General)

4.3.2 文件管制(Control of documents)

4.3.3 紀錄管制(Control of records)

4.3.1一般要求(1)
(General)

文件化應包括管理階層決策的紀錄，確保各項措施可追溯至管理階層決策及政策，並確保所記錄的結果是可再產生的。

能夠展示從所選擇的控制措施回溯至風險評鑑與風險處理過程的結果，且其後能回溯至資訊安全管理系統政策與目標的關係是重要的

4.3.1 一般要求(2) (General)

資訊安全管理系統文件化應包括：

a) 資訊安全管理系統政策(參閱第4.2.1 b)節)與目標之文件化聲明；

b) 資訊安全管理系統之範圍（參閱第4.2.1a)節）；

c) 支援資訊安全管理系統之各項程序與控制措施；

d) 風險評鑑方法(參閱第4.2.1 c)節)的描述；

e) 風險評鑑報告(參閱第4.2.1 c)節至4.2.1 g)節)；

f) 風險處理計畫(參閱第4.2.2 b)節)；

g) 組織爲確保有效規劃、操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 (參閱第4.2.3 c)節)；

h) 本國際標準要求之各項紀錄（參閱第4.3.3節）；及

i) 適用性聲明書。

4.3.2 文件管制 (Control of documents)

資訊安全管理系統所要求之文件應受保護及管制。應建立文件化程序，以界定所需之管理措施，用以：

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鑑別；
d) 確保在使用場所備妥適用文件之相關版本；
e) 確保文件保持易於閱讀並容易鑑別；
f) 確保文件對其需要者可隨時取得，且依據文件之分類以適當的程序予以傳送、儲存及最終處置；
g) 確保外來原始文件已加以鑑別；
h) 確保文件分發已加以管制；
i) 防止失效文件被誤用；及
j) 失效文件若爲任何目的而保留時，應予以適當鑑別。

4.3.3 紀錄管制 (Control of records)

爲提供資訊安全管理系統符合要求及有效運作之證據，應建立並維持各項紀錄。紀錄應加以保護與管制。

資訊安全管理系統應將任何相關的法律或管理要求以及契約義務列入考量。

紀錄應保持易於閱讀，容易鑑別及檢索。紀錄之鑑別、儲存、保護、檢索、保存期限及處置所需的控制措施，應予以文件化並實施。

在第4.2節所述各項過程之績效及所有與資訊安全管理系統有關的重大安全事故，其所發生之紀錄應加以保持。

5. 管理責任
(Management Responsibility)

5.1管理承諾(Management commitment)

5.2資源管理(Resource management)

5.1管理承諾(1)
(Management commitment)

管理階層應藉由下列各項，對資訊安全管理系統之建立、實施、操作、監督、審查、維持與改進之承諾提供證據：

a) 建立一份資訊安全管理系統政策；
b) 確保建立資訊安全管理系統目標及計畫；
c) 爲資訊安全建立角色與職責；
d) 向組織傳達符合資訊安全目標與遵守資訊安全政策、法律規範下之職責以及持續改進需求的重要性；

5.1管理承諾(2)
(Management commitment)

a) 提供充分資源以建立、實施、操作、監督、審查、維持與改進資訊安全管理系統(參閱第5.2.1節)；

b) 決定承受風險與可承受風險等級的準則；

c) 確保執行資訊安全管理系統之內部稽核(參閱第6節)；及

d) 執行資訊安全管理系統之管理階層審查(參閱第7節)。

5.2資源管理
(Resource management)

5.2.1 資源的提供(Provision of resources)

5.2.2 訓練,認知與能力
(Training, awareness and competency)

5.2.1 資源的提供 (Provision of resources)

組織應決定並提供所需的資源，以：

a) 建立、實施、操作、監督、審查、維持及改進資訊安全管理系統；
b) 確保各項資訊安全程序支援營運要求；
c) 鑑別並提出法律與法規要求，以及合約的安全義務；
d) 正確應用所有實施的控制措施，以維護適當之安全；
e) 必要時進行審查，並針對此等審查之結果作適當因應；及
f) 有要求時，改進資訊安全管理系統之有效性。

5.2.2 訓練,認知與能力 (Training, awareness and competency)

組織應確保在資訊安全管理系統中規定負有職責之所有人員，有能力藉由下述執行所要求之工作，包括：

a) 對執行工作會影響資訊安全管理系統之人員，決定其所需的能力；
b) 提供訓練或採取其他措施(如僱用有能力之人員)，以滿足此等需求；
c) 評估所採取措施之有效性；及
d) 維持教育、訓練、技巧、經驗及資格之紀錄（參閱第4.3.3節）。

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，以及他們如何在資訊安全管理系統目標之達成有所貢獻。

6. ISMS內部稽核(1)
(Internal ISMS audit)

組織應在規劃的期間內進行資訊安全管理系統之內部稽核，以決定其資訊安全管理系統之控制目標、控制措施、過程及程序是否：

a) 符合本國際標準及相關法律或法規的要求；
b) 符合所鑑別的資訊安全要求；
c) 有效的實施與維持；及
d) 如預期的執行。

6. ISMS內部稽核(2)
(Internal ISMS audit)

稽核計畫應加以規劃，考慮受稽核的過程與區域之狀況及重要性，以及先前稽核的結果。

稽核準則、範圍、頻率及方法應加以界定。稽核員的選擇與稽核的執行，應確保稽核過程的客觀性與公正性。

稽核員不應稽核其本身的工作。

規劃與執行稽核，以及報告結果與維持紀錄(參閱第4.3.3節)之職責與要求，應以文件化程序加以界定。

受稽核區域負責之管理階層，應確保所採行的措施沒有不當延誤，以消除所發現之不符合與其原因。跟催活動應包括所採行措施之查證與查證結果的報告(參閱第8節)。

7. ISMS之管理階層審查 (Management review of the ISMS)

7.1 概述(General)

7.2 審查輸入(Review input)

7.3 審查輸出(Review output)

7.1 概述(General)

管理階層應在規劃的期間內(至少一年一次)，審查組織的資訊安全管理系統，以確保其持續的適用性、適切性及有效性。

此項審查應包括改進機會與資訊安全管理系統變更需求的評核，包括資訊安全政策與資訊安全目標。

審查結果應予清楚的文件化，且紀錄應予以維持(參閱第4.3.3節)。

7.2 審查輸入(Review input)

管理階層審查之輸入應包括：

a) 資訊安全管理系統稽核與審查之結果；
b) 來自利害相關者之回饋；
c) 可用以改進組織資訊安全管理系統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) 先前風險評鑑未適切提出之脆弱性或威脅；
f) 有效性量測的結果；
g) 先前管理階層審查之跟催措施；
h) 可能影響資訊安全管理系統之任何變更；及
i) 改進之建議

7.3 審查輸出(Review output)

管理階層審查之輸出應包括下列有關之任何決定與措施：

a) 資訊安全管理系統有效性之改進。

b) 風險評鑑與風險處理計畫之更新。

c) 爲因應可能衝擊資訊安全管理系統之內部或外部事件，必要時，影響資訊安全之程序與控制措施應予以修訂，包括下列事項之變動：

   1) 營運要求；

   2) 安全要求；

   3) 影響既有營運要求之營運過程；

   4) 法規或法律要求；

   5) 合約的義務；及

   6) 風險等級及/或風險承受準則。

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(ISMS improvement)

8.1持續改進(Continual improvement)

8.2矯正措施(Corrective action)

8.3預防措施(Preventive action)

8.1持續改進(Continual improvement)

組織應藉由資訊安全政策、資訊安全目標、稽核結果、監督事件之分析、矯正與預防措施以及管理階層審查(參閱第7節)之使用，以持續改進資訊安全管理系統之有效性。

8.2矯正措施(Corrective action)

爲防止再發，組織應採取措施，以消除與資訊安全管理系統要求不符合之原因。矯正措施的文件化程序應界定各項要求，以:

a) 鑑別不符合；
b) 決定不符合之原因；
c) 評估措施之需求，以確保不符合不再發生；
d) 決定與實施所需之矯正措施；
e) 記錄採取措施的結果(參閱第4.3.3節)；及
f) 審查所採取措施。

8.3預防措施(Preventive action)

組織應決定措施，以消除與資訊安全管理系統要求潛在不符合之原因，防止其發生。所採取之預防措施應與潛在問題之衝擊相稱。

預防措施之文件化程序應界定各項要求，以：

a) 鑑別潛在的不符合與其原因；
b) 評估措施的需求，以防止不符合的發生；
c) 決定與實施所需之預防措施；
d) 記錄所採取措施之結果(參閱第4.3.3節)；及
e) 審查所採取措施。

組織應鑑別已變更之風險，以及鑑別預防措施之要求並特別注意重大變更之風險。預防措施之優先順序應依據風險評鑑之結果加以決定。

ISO27001 2005和2013版本差異

2005 年版本條款			2013 年版本條款		
0.	簡述 Introduction		0.	簡述 Introduction	
1.	範圍 (Scope)		1.	範圍 (Scope)	
2.	引用標準 (Normative references)		2.	引用標準 (Normative references)	
3.	用語釋義 (Terms and definitions)		3.	用語釋義 (Terms and definitions)	
4.	資訊安全管理(Information security management) system	(Plan)	4.	組織全景(Context of the organization)	(Plan)
	-		5.	領導力 (Leadership)	(Plan)
	-		6.	規劃 (Planning)	(Plan)
	-		7.	支援 (Support)	(Plan)
5.	管理階層責任(Management responsibility)	(Do)	8.	運作 Operation	(Do)
6.	ISMS 內部稽核(Internal ISMS audits) (Check)			-	
7.	ISMS 之管理審查（Management review of the ISMS ）	(Check)	9.	績效評估(Performance evaluation)	(Check)
8.	ISMS 之改進 (ISMS improvement)	(Act)	10.	改進(Improvement)	(Act)

Documented information

The requirements for documented information are spread throughout the standard. However, in summary they are:

4.3	Scope of the ISMS
5.2	Information security policy
6.1.2	Information security risk assessment process
6.1.3	Information security risk treatment process
6.1.3 d)	Statement of Applicability
6.2	Information security objectives
7.2 d)	Evidence of competence
7.5.1 b)	Documented information determined by the organization as being necessary for the effectiveness of the ISMS
8.1	Operational planning and control
8.2	Results of the information security risk assessments
8.3	Results of the information security risk treatment
9.1	Evidence of the monitoring and measurement results
9.2 g)	Evidence of the audit programme(s) and the audit results
9.3	Evidence of the results of management reviews
10.1 f)	Evidence of the nature of the nonconformities and any subsequent actions taken
10.1 g)	Evidence of the results of any corrective action

Clause 0: Introduction

- This is a much shorter clause than its predecessor. In particular the
- section on the PDCA model has been removed. The reason for this is
- that the requirement is for continual improvement (see Clause 10)
- and PDCA is just one approach to meeting that requirement. There
- are other approaches, and organizations are now free to use them if
- they wish.
- The introduction also draws attention to the order in which
- requirements are presented, stating that the order does not reflect
- their importance or imply the order in which they are to be
- implemented.

Clause 1: Scope

- This, too, is a much shorter clause. In particular there is no reference to the exclusion of controls in Annex A.

Clause 2: Normative references

- The only normative reference is to ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary.

Clause 3: Terms and definitions

- There are no longer any terms or definitions in ISO/IEC 27001:2013. Instead, readers are referred to ISO/IEC 27000. However, please ensure that you use a version of ISO/IEC 27000 that was published after ISO/IEC 27001:2013 otherwise it will not contain the correct terms or definitions.
- This is an important document to read. Many definitions, for example ‘management system’ and ‘control’ have been changed and now conform to the definitions given in the new ISO directives and ISO 31000. If a term is not defined in ISO/IEC 27000, please use the definition given in the Oxford English Dictionary. This is important, otherwise confusion and misunderstanding may be the result.

Clause 4: Context of the organization

- This is a new clause that in part addresses the depreciated concept of preventive action and in part establishes the context for the ISMS. It meets these objectives by drawing together relevant external and internal issues (i.e. those that affect the organization's ability to achieve the intended outcome(s) of its ISMS) with the requirements of interested parties to determine the scope of the ISMS.
- It should be noted that the term 'issue' covers not only problems, which would have been the subject of preventive action in the previous standard, but also important topics for the ISMS to address, such as any market assurance and governance goals that the organization might set for the ISMS. Further guidance is given in Clause 5.3 of ISO 31000:2009.
- Note that the term 'requirement' is a 'need or expectation that is stated, generally implied or obligatory'. Combined with Clause 4.2, this in itself can be thought of as a governance requirement, as strictly speaking an ISMS that did not conform to generally-accepted public expectations could now be ruled nonconformant with the standard.
- The final requirement (Clause 4.4) is to establish, implement, maintain and continually improve the ISMS in accordance with the requirements the standard.

Clause 5: Leadership

- This clause places requirements on ‘top management’ which is the person or group of people who directs and controls the organization at the highest level. Note that if the organization that is the subject of the ISMS is part of a larger organization, then the term ‘top management’ refers to the smaller organization. The purpose of these requirements is to demonstrate leadership and commitment by leading from the top.
- A particular responsibility of top management is to establish the information security policy, and the standard defines the characteristics and properties that the policy is to include.
- Finally, the clause places requirements on top management to assign information security relevant responsibilities and authorities, highlighting two particular roles concerning ISMS conformance to ISO/IEC 27001 and reporting on ISMS performance

Clause 6: Planning

- Clause 6.1.1, General:
  - This clause works with Clauses 4.1 and 4.2 to complete the new way of dealing with preventive actions. The first part of this clause (i.e. down to and including 6.1.1 c)) concerns risk assessment whilst Clause 6.1.1 d) concerns risk treatment. As the assessment and treatment of information security risk is dealt with in Clauses 6.1.2 and 6.1.3, then organizations could use this clause to consider ISMS risks and opportunities.

- Clause 6.1.2, Information security risk assessment:
  - This clause specifically concerns the assessment of information security risk. In aligning with the principles and guidance given in ISO 31000, this clause removes the identification of assets, threats and vulnerabilities as a prerequisite to risk identification. This widens the choice of risk assessment methods that an organization may use and still conforms to the standard. The clause also refers to ‘risk assessment acceptance criteria’, which allows criteria other than just a single level of risk. Risk acceptance criteria can now be expressed in terms other than levels, for example, the types of control used to treat risk.
  - The clause refers to ‘risk owners’ rather than ‘asset owners’ and later (in Clause 6.1.3 f)) requires their approval of the risk treatment plan and residual risks.
  - In other ways the clause closely resembles its counterpart in ISO/IEC 27001:2005 by requiring organizations to assess consequence, likelihood and levels of risk

- Clause 6.1.3, Information security risk treatment:
  - This clause concerns the treatment of information security risk. It is similar to its counterpart in ISO/IEC 27001:2005, however, it refers to the ‘determination’ of necessary controls rather than selecting controls from Annex A. Nevertheless, the standard retains the use of Annex A as a cross-check to make sure that no necessary control has been overlooked, and organizations are still required to produce a Statement of Applicability (SOA). The formulation and approval of the risk treatment plan is now part of this clause.

- Clause 6.2, Information security objectives and planning to achieve them:
  - This clause concerns information security objectives. It uses the phrase “relevant functions and levels”, where here, the term ‘function’ refers to the functions of the organization, and the term ‘level’, its levels of management, of which ‘top management’ is the highest. The clause defines the properties that an organization’s information security objectives must possess.

Clause 7: Support

- This clause begins with a requirement that organizations shall determine and provide the necessary resources to establish, implement, maintain and continually improve the ISMS. Simply expressed, this is a very powerful requirement covering all ISMS resource needs.
- The clause continues with requirements for competence, awareness and communication, which are similar to their counterparts in ISO/IEC 27001:2005.
- Finally, there are the requirements for ‘documented information’. ‘Documented information’ is a new term that replaces the references in the 2005 standard to ‘documents’ and ‘records’. These requirements relate to the creation and updating of documented information and to their control. The requirements are similar to their counterparts in ISO/IEC 27001:2005 for the control of documents and for the control of records.
- Note that the requirements for documented information are presented in the clause to that they refer to. They are not summarized in a clause of their own, as they are in ISO/IEC 27001:2005.

Clause 8: Operation

- This clause deals with the execution of the plans and processes that are the subject of previous clauses.
  - **Clause 8.1** deals with the execution of the actions determined in Clause 6.1, the achievement of the information security objectives and outsourced processes;
  - **Clause 8.2** deals with the performance of information security risk assessments at planned intervals, or when significant changes are proposed or occur; and
  - **Clause 8.3** deals with the implementation of the risk treatment plan.

Clause 9: Performance evaluation

- **Clause 9.1**, Monitoring, measurement, analysis and evaluation:
  - The first paragraph of Clause 9.1 states the overall goals of the clause. As a general recommendation, determine what information you need to evaluate the information security performance and the effectiveness of your ISMS. Work backwards from this 'information need' to determine what to measure and monitor, when, who and how. There is little point in monitoring and making measurements just because your organization has the capability of doing so. Only monitor and measure if it supports the requirement to evaluate information security performance and ISMS effectiveness.
  - Note that an organization may have several information needs, and these needs may change over time. For example, when an ISMS is relatively new, it may be important just to monitor the attendance at, say, information security awareness events. Once the intended rate has been achieved, the organization might look more towards the quality of the awareness event. It might do this by setting specific awareness objectives and determining the extent to which the attendees have understood what they have learnt. Later still, the information need may extend to determine what impact this level of awareness has on information security for the organization.

- **Clause 9.2**, Internal audit:
  - This clause is similar to its counterpart in ISO/IEC 27001:2005. However, the requirement holding management responsible for ensuring that audit actions are taken without undue delay has been removed, as it is effectively covered by the requirements in Clause 10.1 (in particular 10.1 a), c) and d)). The requirement that auditors shall not audit their own work has also been removed, as it is covered by the requirement to ensure objectivity and impartiality (Clause 9.2 e)).
- **Clause 9.3**, Management review:
  - Rather than specify precise inputs and outputs, this clause now places requirements on the topics for consideration during the review. The requirement for reviews to be held at planned intervals remains but the requirement to hold the reviews at least once per year has been dropped.

Clause 10: Improvement

- Due to the new way of handling preventive actions, there are no preventive action requirements in this clause. However, there are some new corrective action requirements. The first is to react to nonconformities and take action, as applicable, to control and correct the nonconformity and deal with the consequences. The second is to determine whether similar nonconformities exist, or could potentially occur. Although the concept of preventive action has evolved there is still a need to consider potential nonconformities, albeit as a consequence of an actual nonconformity. There is also a new requirement to ensure that corrective actions are appropriate to the effects of the nonconformities encountered.
- The requirement for continual improvement has been extended to cover the suitability and adequacy of the ISMS as well as its effectiveness, but it no longer specifies how an organization achieves this.

Annex A

- The title of Annex A is now “reference control objectives and controls” and the introduction is simplified. It states that the control objectives and controls are directly derived from ISO/IEC 27002:2013 and that the Annex is to be used in the context of Clause 6.1.3.
- During the revision of ISO/IEC 27002 the number of controls has been reduced from 133 controls to 114 controls, and the number of major clauses has been expanded from 11 to 14. Some controls are identical or otherwise very similar; some have been merged together; some have been deleted and some are new. For example:
  1. A.5.1.1, Policies for information security is very similar to the original A.5.1.1, Information security policy document.
  2. The old A.10.10.1, Audit logging, A.10.10.2, Monitoring of system use, and A.10.10.5, Fault logging, have been merged together to form the new A.12.4.1, Event logging.
  3. The old A.11.6.2, Sensitive system isolation, has been removed on the grounds that in an interconnected world, such a control defeats the objective of being interconnected.
  4. A.17.2.1, Availability of information processing facilities is a new control.

- It is important to appreciate that the usefulness of a control to an organization should not change because it has been removed from Annex A. In accordance with Clause 6.1.3, controls are now determined on the basis of risk treatment. If an organization wishes to treat particular risks by deliberately not connecting a computer to the Internet or other networks, then it will need to use a control like the old A.11.6.2 regardless of whether it is in Annex A or not.
- Annex A remains as a ‘normative annex’. This is not because Annex A contains normative requirements but because, by ISO rules, it is referenced from a normative requirement, i.e. in this case, Clauses 6.1.3 c) and d).

Other annexes

- The original Annex B, OECD principles and this international standard, has been dropped as it is now an old reference, which refers to PDCA.
- The old Annex C, Correspondence between ISO 9001:2000, ISO 14001:2004 and this international standard, has also been dropped because both of these standards are being revised and will use the same high level structure and identical core text as ISO/IEC 27001:2013.
- Annex B, Bibliography, of ISO/IEC 27001:2013 is an updated version of its counterpart, Annex D in ISO/IEC 27001:2005.