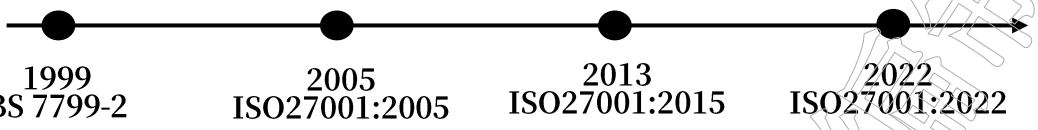
ASFALIS INTERNATIONAL
艾斯飛利國際有限公司

ISO27001:2022 Gap Analysis (External Use)

ISO27001沿革
History



名稱差異
Name of the standards

ISO27001:2013	ISO27001:2022
資訊技術-安全技術-資訊安全管理系統-要求事項 Information technology - Security techniques– Information security management systems – Requirements	**資訊安全、網路安全及隱私保護**-資訊安全管理系統-要求事項 Information security, Cybersecurity and privacy Protection– Information security management systems – Requirements
114個控制措施 security controls in Annex A	**93**個控制措施 security controls in Annex A
14個控制領域 14 areas	**4**大主題 4 domains

本文差異
Changes in chapter 4 through 10

ISO27001:2022			ISO27001:2013	
章節	控制項	內容	章節	控制項
4	**組織全景**			
4.2	了解利益團體的需求與期望	組織須確認： (a) 與資訊安全系統相關的利益團體。 (b) 利益團體的相關要求。 **(c) 前述要求應在資訊安全管理系統中被妥善處理。**	4.2	組織須確認： a) 與資訊安全系統相關的利益團體。 b) 利益團體對資訊安全的要求。

Add

c) which of these requirements will be addressed through the information security management system.

ISO27001:2022 Gap Analysis (External Use)

艾斯飛利國際有限公司

ISO27001:2022			ISO27001:2013	
章節	控制項	內容	章節	控制項
4	**組織全景**			
4.4	資訊安全管理系統	組織須建立、實作、維持及持續改善資訊安全管理系統，**包括依據本文件所要求程序與互動**。	4.4	組織須建立、實作、維持及持續改善資訊安全管理系統。

Add “including the processes needed and their interactions,”

5	**領導力**			
5.3	組織的角色、責任與職權	最高管理階層應確保資訊安全相關角色之責任及權限已指派並**向組織內部**傳達。 最高管理階層應指派下列責任及權限。 (a) 確保資訊安全管理系統符合本文件之要求事項。 (b) 向最高管理階層報告資訊安全管理系統之績效。	組織的角色、責任與職權	最高管理階層應確保資訊安全相關角色之責任及權限已指派並傳達。 最高管理階層應指派下列責任及權限。 (a) 確保資訊安全管理系統符合本文件之要求事項。 (b) 向最高管理階層報告資訊安全管理系統之績效。

Add within the organization

6	**計畫**			
6.3	變更計畫	當組織確定需要變更資訊安全管理時系統，變更應有計劃地進行。		

Add When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

7	**支持**			
7.4	溝通	組織應決定，相關於資訊安全管理系統之內部及外部溝通或傳達的需要，包括下列事項。 (a) 溝通或傳達事項。 (b) 溝通或傳達時間。 (c) 溝通或傳達對象。 **(d) 如何傳達**。	7.4	組織應決定，相關於資訊安全管理系統之內部及外部溝通或傳達的需要，包括下列事項。 (a) 溝通或傳達事項。 (b) 溝通或傳達時間。 (c) 溝通或傳達對象。 (d) 溝通或傳達人員。 (e) 進行有效溝通或傳達所採取之過程。

CHANGE d) how to communicate. ← d) who shall communicate; and e) the processes by which communication shall be affected.

ASFALIS INTERNATIONAL
艾斯飛利國際有限公司

ISO27001:2022 Gap Analysis (External Use)

ISO27001:2022			ISO27001:2013	
章節	控制項	內容	章節	控制項
8	營運作業			
8.1	營運規劃與控制	組織應規劃、實作及控制達成資訊安全要求事項所需之過程，並透過以下方式實作第6章中所決定之行動： 為這些過程設置規範(criteria)；依據這些規範實施控制。 組織應控制所規劃之變更，並審查非預期變更之後果，必要時採取行動以減輕任何負面效果。 文件化資訊應能被取得(available)，其程度必須具有足以達成其過程已依規劃執行之信心。 組織應確保與資訊安全管理系統有關之外來程序、產品或服務受控制。	8.1	組織應規劃、實作及控制達成資訊安全要求事項所需之過程，並實作6.1中所決定之行動 組織亦應實作各項計畫，以達成6.2 中所決定之資訊安全目標。 組織應保存文件化資訊，其程度必須具有足以達成其過程已依規劃執行之信心。

CHANGE

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

establishing criteria for the processes;

implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.

The organization shall also implement plans to achieve information security objectives determined in 6.2.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

ASFALIS INTERNATIONAL

艾斯飛利國際有限公司

ISO27001:2022 Gap Analysis (External Use)

ISO27001:2022			ISO27001:2013	
章節	控制項	內容	章節	控制項
9	績效評量			
9.3	管理審查		9.3	管理審查 最高管理階層應於規劃之期間，審查組織之資訊安全管理系統，以確保其持續的合宜性、適切性及有效性。 管理審查應包括對下列事項之考量。 (a) 過往管理審查之議案的處理狀態。 (b) 與資訊安全管理系統有關之內部及外部議題的變更。 (c) 資訊安全績效之回饋，包括下列之趨勢。 (1) 不符合項目及矯正措施。 (2) 監督及量測結果。 (3) 稽核結果。 (4) 資訊安全目標之達成。 (d) 關注方之回饋。 (e) 風險評鑑結果及風險處理計畫之狀態。 (f) 持續改善之機會。 管理審查之輸出應包括與持續改善機會有關之決策，以及任何對資訊安全管理系統變更之需要。 組織應保存文件化資訊，以作為管理審查結果之證據。
9.3.1	概述	最高管理階層應於規劃之期間，審查組織之資訊安全管理系統，以確保其持續的合宜性、適切性及有效性。		
9.3.2	管理審查輸入項	管理審查應包括考慮： (a) 過往管理審查之議案的處理狀態； (b) 與資訊安全管理系統有關之內部及外部議題的變更; (c) 與資訊安全管理系統有關之**關注方需求和期望變化**； (d) 資訊安全績效之回饋，包括下列之趨勢： (1) 不符合項目及矯正措施； (2) 監測和測量結果； (3) 稽核結果； (4) 資訊安全目標的實現； (e) 關注方的反饋； (f) 風險評鑑結果及風險處理計畫之狀態； (g) 持續改善之機會。		
9.3.3	管理審查輸出項	管理審查之輸出應包括與持續改善機會有關之決策，以及任何對資訊安全管理系統變更之需要。 組織應保存文件化資訊，以作為管理審查結果之證據。		

Add

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

CHANGE

Structural changes

ISO27001:2022 Gap Analysis (External Use)

艾斯飛利國際有限公司

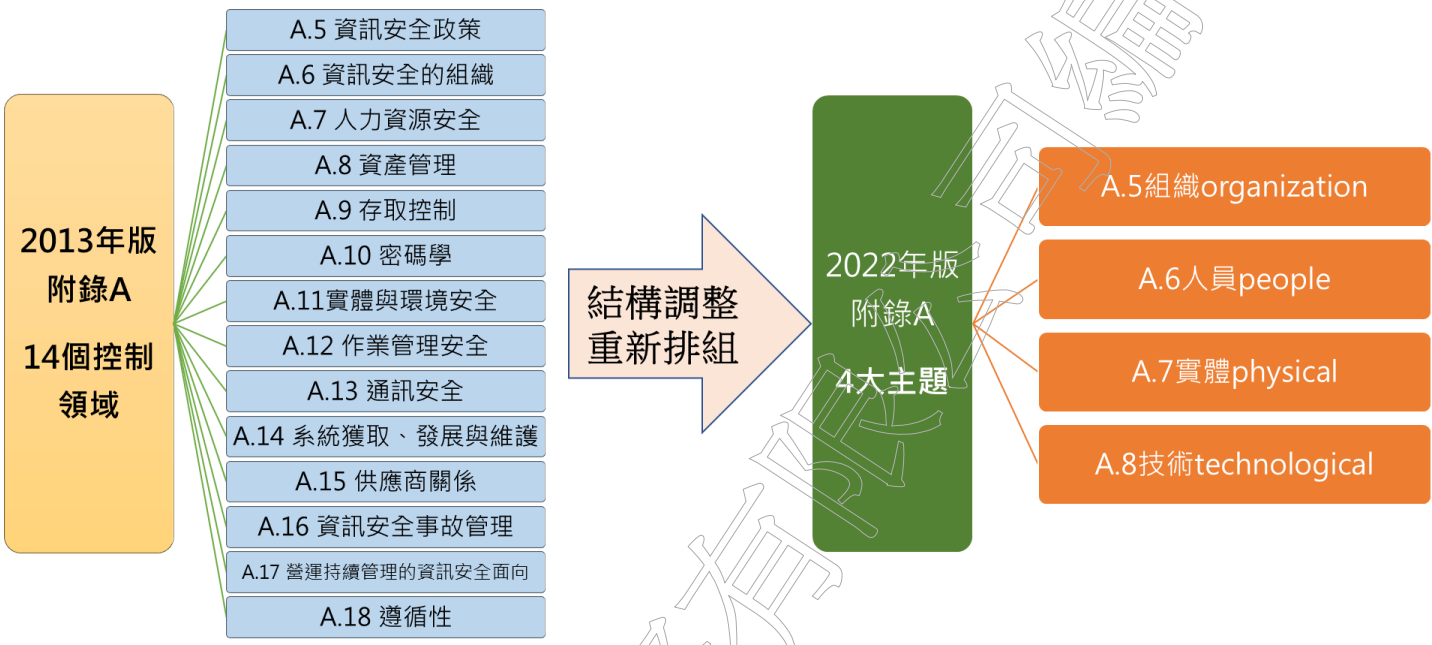
ISO27001:2022			ISO27001:2013	
章節	控制項	內容	章節	控制項
10	**改善**			
10.1	持續改善	組織應持續改善資訊安全管理系統之合宜性、適切性及有效性。	10.1	不符合事項與矯正措施 不符合項目發生時，組織應有下列作為。 (a) 對不符合項目反應，並於適當時採取下列作為。 (1) 採取行動以控制並矯正之。 (2) 處理其後果。 (b) 藉由下列作為，評估對消除不符合項目之原因的行動之需要，使其不再發生且不於他處發生。 (1) 審查不符合項目。 (2) 決定不符合項目之原因。 (3) 決定是否有類似之不符合項目存在，或可能發生。 (c) 實作所有所需行動。 (d) 審查所有所採取矯正措施之有效性。 (e) 若必要時，則對資訊安全管理系統進行變更。 矯正措施應切合所遇到之不符合項目。 組織應保存文件化資訊，以作為下列事項之證據。 (f)不符合項目之本質及後續採取之所有行動。 (g) 所有矯正措施之結果。
10.2	不符合事項與矯正措施	不符合項目發生時，組織應有下列作為。 (a) 對不符合項目反應，並於適當時採取下列作為。 (1) 採取行動以控制並矯正之。 (2) 處理其後果。 (b) 藉由下列作為，評估對消除不符合項目之原因的行動之需要，使其不再發生且不於他處發生。 (1) 審查不符合項目。 (2) 決定不符合項目之原因。 (3) 決定是否有類似之不符合項目存在，或可能發生。 (c) 實作所有所需行動。 (d) 審查所有所採取矯正措施之有效性。 (e) 若必要時，則對資訊安全管理系統進行變更。 矯正措施應切合所遇到之不符合項目。 文件化資訊應能被取得(available)，以做為下列事項之證據。 (f)不符合項目之本質及後續採取之所有行動。 (g) 所有矯正措施之結果。	10.2	持續改善 組織應持續改善資訊安全管理系統之合宜性、適切性及有效性。

CHANGE Structural changes

ASFALIS INTERNATIONAL
艾斯飛利國際有限公司

ISO27001:2022 Gap Analysis (External Use)

附錄A差異
Annex A - Controls:



改變程度changes		
重大變更(新內容) Major	11個新控制項 11 new controls	
中等 Moderate	其中57個 併為 24個； 57 merged into 24	其中1個分為2個 1 divided into 2
輕度	23個改名 23 renamed	
無變化	35個不變 35 remained the same	

ASFALIS INTERNATIONAL

艾斯飛利國際有限公司

ISO27001:2022 Gap Analysis (External Use)

新控制措施
New controls clause no. and description

A.5.7 威脅情報(Threat intelligence)

1. 控制措施

應蒐集並分析有關資訊安全威脅之相關資訊，進而產出情報。

2. 目的

提供對組織環境威脅的意識，以便採取適當行動。

5.7 Threat intelligence
Information relating to information security threats shall be collected and analysed to produce threat intelligence.

A.5.23 雲端服務與資訊安全 (Information security for use of cloud services)

1. 控制措施

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。

2. 目的

為雲端服務之使用，具體說明及管理資訊安全。

5.23 Information security for the use of cloud services
Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.

A.5.30營運持續之資通訊準備 (ICT readiness for business continuity)

1. 控制措施

應根據業務連續性目標以及資通訊連續性要求，規劃、實施、維護、測試資通訊準備(ICT readiness)。

2. 目的

在服務中斷期間，確保組織的資訊和其他相關資產之可用性。

5.30 ICT readiness for business continuity
ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

A.7.4實體安全監控(Physical security monitoring)

1. 控制措施

應持續監控營運場所(Premises)是否存在未經授權的實體進出(physical access)。

2. 目的

檢測並阻止未經授權的實體進出。

7.4 Physical security monitoring
Physical security for offices, rooms and facilities shall be designed and implemented.

ASFALIS INTERNATIONAL

艾斯飛利國際有限公司

ISO27001:2022 Gap Analysis (External Use)

新控制措施
New controls clause no. and description

A.8.9組態管理 (Configuration management)

1. 控制措施

應建立、文件化、實施、監控和審查，包含有關硬體、軟體、服務、網路等安全組態。

2. 目的

確保硬體、軟體、服務、網路正常運行並具安全性設置，並且組態不會因未經授權或不正確的變更而改變。

8.9 Configuration management
Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.

A.8.10資訊刪除 (Information deletion)

1. 控制措施

當儲存在資訊系統、設備、其他儲存媒體的資訊不需要時，應將其刪除。

2. 目的

防止非必要敏感資訊洩露，並遵守法律、法規、資訊刪除的監管和合約要求。

8.10 Information deletion
Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.

A.8.11資料遮罩(Data masking)

1. 控制措施

應根據組織的特定主題訪問策略使用資料遮罩，控制和其他相關的特定主題的政策和業務要求，並將適用的法律納入考慮。

2. 目的

限制敏感資料的曝光(exposure)，如個人可識別資訊(personally identifiable information, PII)，並遵守法律、法規、監管、合約要求。

8.11 Data masking
Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

A.8.12資料外洩防範(Data leakage prevention)

1. 控制措施

數據外洩防範應應用於系統、網路，以及其他處理、存儲或傳送敏感資訊的設備。

2. 目的

檢測並防止未經授權之揭露和存取資訊。

8.12 Data leakage prevention
Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.

ISO27001:2022 Gap Analysis (External Use)

艾斯飛利國際有限公司

新控制措施
New controls clause no. and description

A.8.16活動監控 (Monitoring activities)

1. 控制措施

應監控網路、系統和應用程序的異常徵候(behaviour)並採取適當的措施，評估潛在資訊安全事件。

2. 目的

偵測異常行為和潛在的資訊安全事件。

8.16 Monitoring activities
Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

A.8.23網頁安全防護 (Web filtering)

1. 控制措施

應管理對外部網站的存取，以減少對惡意內容的接觸。

2. 目的

保護系統免受惡意軟體的破壞、避免存取未經授權的網路資源。

8.23 Web filtering
Access to external websites shall be managed to reduce exposure to malicious content.

A.8.28程式開發安全 (Secure coding)

1. 控制措施

程式開發安全原則應運用於軟體開發。

2. 目的

減少潛在資訊安全漏洞的數量。

8.28 Secure coding
Secure coding principles shall be applied to software development.

轉版時程
Transition period

Companies certified against the 2013 revision must transition to the 2022 revision by October 31, 2025 (3-year period)