eBook

符合ISO/IEC 27001:2022資料安全合規性——資訊安全、網路安全與隱私保護標準

Thales解決方案如何協助實現ISO/IEC 27001合規要求

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

ISO（國際標準化組織）是一個獨立的、非政府的國際組織，擁有170個會員國家標準機構。ISO/IEC 27001由ISO與國際電工委員會（IEC）共同發布，是全球最知名的資訊安全管理系統（ISMS）標準。ISO/IEC 27001標準為所有組織提供了建立、實施、維護和持續改善資訊安全管理系統的指導。

符合 ISO/IEC 27001 表示該組織或企業已經建立了一套系統，來管理組織/企業擁有或處理的資料安全相關的風險，並且該系統採用該國際標準中規範的所有最佳實踐和原則。

ISO/IEC 27001 最新版本有哪些修訂?

ISO/IEC 27001 首次於 2005 年發布，於 2013 年 9 月 25 日修訂為 ISO/IEC 27001:2013，並於 2022 年 10 月 25 日再次修訂為 ISO/IEC 27001:2022。 該標準不段更新，以反應技術和資訊安全不斷變化的需求。 2022 年最大的變化是附錄 A。

ISO/IEC 27001 中的附錄 A 是該標準的一部分，條列組織用來證明符合 ISO/IEC 27001 6.1.3（資訊安全風險處理）的一組分類安全控制措施。 ISO/IEC 27002:2013 總共合併了 24 項控制措施，修訂了 58 項控制措施，使其與當前的網路安全和資訊安全環境保持一致。

	ISO/IEC 27001: 2013	ISO/IEC 27001: 2022
附錄 A 控制類別	114個控制 14部分	93個控制 4個部分 • 組織 – 37個控制 • 人員 – 8個控制 • 硬體 – 14個控制 • 技術 – 34個控制

哪些公司可以獲得 ISO/IEC 27001:2022 認證?

ISO 標準獲得國際網路安全專家的認可，並獲得全球廣泛認可。 ISO 認證適用於所有經濟部門的組織，包括各種服務業和製造業以及基礎產業部門，不分私營、公共和非營利組織。

不遵守 ISO/IEC 27001:2022 法規，將受到哪些處分?

ISO/IEC 27001是一個國際標準，對於不符合標準並不會受到處分。然而，ISO/IEC 27001:2022認證可以在資料違規事件中提供組織一個保障，例如GDPR等法規可能對於資料違規會施加罰款，組織通過提出實施資訊安全標準方面的最佳實踐證明，可以展示組織對法規遵循的努力。

Thales 如何協助實現 ISO/IEC 27001:2022 合規性?

Thales 透過滿足附錄 A 中所有的資訊安全控制的基本要求，幫助組織遵守 ISO/IEC 27001:2022。

ISO/IEC 27001:2022 Requirements	Thales Solutions
資訊分類	
5.12: 資訊分類: 資訊應根據資訊安全需求進行分類。	CipherTrust Data Discovery and classification 可識別公司內部和雲端中的結構化和非結構化機敏資料。 內建範本可以快速識別受監管的資料、凸顯安全風險並協助發現合規性漏洞。
資料安全	
5.3: 職責分離 應該區隔相互衝突的職責和相互衝突的責任。 **5.33: 記錄保護** 應保護記錄免遭遺失、破壞、偽造、未經授權的存取和未經授權的發布。 **5.34: 個人隱私和個人身份資訊（PII）的保護** 根據適用的法律法規和合約要求，確定並滿足有關保護隱私和保護個人身份資訊的要求。 **8.7: 防範惡意軟體** 應實施防範惡意軟體的措施，並由適當的用戶意識支援和配合。 **8.10: 資訊刪除** 資料不再需要使用時，應該刪除儲存在資訊系統、設備或任何其他儲存媒介中的資訊。 **8.11: 資料遮罩** 應根據組織的特定主題政策，如存取控制和其他相關主題政策，來使用資料遮罩。 **8.12: 資料外洩防護** 在處理、儲存或傳輸敏感資訊的系統、網路和任何其他設備上應用資料外洩預防措施。 **8.24: 密碼學的使用** 應定義和實施有效使用密碼學的規則，包括密碼金鑰管理。	CipherTrust Data Security Platform 提供多種功能來保護文件、磁碟區和資料庫中的靜態資料。 其中包括： • CipherTrust **透明加密**透過集中金鑰管理和特權使用者存取控制提供靜態資料加密。 它提供完全的角色分離，只有授權的使用者和程序才能查看未加密的資料。 這可以確保隱私並保護機敏資料，無論資料在本地、跨多個雲端、大數據和容器環境中。 • 具有動態資料遮罩的CipherTrust Tokenization 允許對資料庫中的機敏資訊進行假名化，同時保留分析聚合資料的能力，而不會在分析期間或報告中暴露機敏資料。 • CipherTrust Enterprise Key Management 透過多種應用案例簡化並加強雲端和企業環境中的金鑰管理。 採用符合 FIPS 140-2 的虛擬或硬體設備，Thales 金鑰管理工具和解決方案，為機敏環境提供高安全性，並集中管理內部加密和第三方應用程式集中的金鑰。 此外，透過銷毀加密金鑰可確保有效地刪除加密訊息。 • CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) 持續監控進程中的異常 I/O 活動，並在勒索軟體完全控制您的端點和伺服器之前，發出警報或阻止惡意活動。 它監控活動程序以檢測勒索軟體，識別過度資料存取、洩漏、未經授權的加密或惡意冒充用戶等，並在檢測到此類活動時發出警報並封鎖。 Thales Luna Hardware Security Modules (HSMs) 保護加密金鑰，並提供符合 FIPS 140-3 Level 3之強化、防篡改環境，以實現安全密碼處理、金鑰產生和保護、加密等。 Luna HSM 可在本地、雲端即服務以及混合環境中使用。 Luna HSM包括： 生成並保護根憑證和憑證授權中心 (CA) 金鑰，為各種應用的 PKI 提供支援 • 應用程式代碼簽章，以確保軟體始終維持安全、未被更改且真實出處。 • 為物聯網應用和其他網路部署建立數位證書，用於專有電子設備賦與設備憑證和驗證。 Thales High Speed Encryptors (HSEs) 提供獨立於網路的動態資料加密（第 2 、 3 和 4 層），確保資料在站點之間、或在本地與雲端之間傳輸的安全。 我們的網路加密解決方案可幫助客戶防止資料洩漏，在不影響效能下，更佳地保護資料、影片、語音和詮釋資料避免遭竊聽、監視以及公開和隱藏的攔截。

ISO/IEC 27001:2022 Requirements	Thales Solutions
存取控制和身份認證	
5.15: 存取控制 應建立並實施對資訊和其他相關資產的實體和邏輯存取的控制規則。 **5.17: 認證資訊** 認證資訊的分配和管理應由管理流程控制。 **5.18: 存取權** 應根據政策規定、審查、修改和刪除資訊存取權。 **6.7: 遠距工作** 人員遠距工作時應採取安全措施。 **8.3: 資訊存取限制** 應根據已製定的特定主題的存取控制政策，限制對資訊和其他相關資產的存取。 **8.4: 存取原始碼** 應管理對原始程式碼、開發工具和軟體庫的讀寫存取。 **8.5: 安全認證** 應實施安全認證技術和流程。	Thales OneWelcome identity and access management solutions 依據內部和外部使用者的角色和上下文，限制其存取。 在強身份驗證 (MFA) 的支援下，精細的存取策略和細膩的授權策略，有助於確保正確的使用者，在正確的時間獲得對正確資源的存取權限。 這高效地降低未經授權存取的風險。 • SafeNet Trusted Access是以雲端為基礎的存取管理解決方案，提供商業化、現成的多因素身份驗證以及最廣泛的硬體和軟體身份驗證方法和形式。 • Thales converged badge solutions 透過將所有企業安全應用程式，整合到單一用戶識別中，簡化了實體和邏輯存取的管理：包括對建築物和限制區域的實體門禁管制、對持卡人的證件識別、基於PKI 憑證和/或 FIDO 身份驗證，對機敏數位資源的安全存取。 • **可支援身份認證**的方法眾多，可滿足各種使用者的需求，並使企業能透過強大的多因素身份驗證來保護所有使用者和機敏數位資源。 Thales OneWelcome Consent & Preference Management 模組，使企業能收集經過終端消費者認可的選項，因此，如金融機構可以清楚地了解業經同意的資料，進而管理被允許他們使用的資料存取權限。 CipherTrust Transparent Encryption 可對機敏資料進行加密，並強制執行可依使用者、流程、檔案類型、時間和其他參數套用的精細特權使用者存取管理策略。 它提供完全的角色分離，只有授權的使用者和程序才能查看未加密的資料。
雲端安全	
5.23: 使用雲端服務的資訊安全 應建立雲端服務的取得、使用、管理和退出流程。 **5.30: 資訊通訊技術（ICT）為企業永續營運最好準備** 應根據業務永續性的目標來計劃、實施、維護和測試ICT的準備工作。	CipherTrust Cloud Key Manager 可以在組織的完全控制下維護本機金鑰，以保護「自帶金鑰」(BYOK) 系統下第三方雲端提供者託管的機敏資料，進而降低第三方雲端安全風險。 CipherTrust Transparent Encryption 提供管理角色的完全分離，只有授權使用者和程序才能查看未加密的資料。 除非提供存取資料的正當理由，否則未經授權的使用者，將無法以明文形式存取儲存在第三方雲端中的機敏資料。 Thales Data Security solutions 解決方案提供最全面的資料保護，如Thales Data Protection on Demand (DPoD)，它為基於雲端的 Luna Cloud HSM 和 CipherTrust Key Management 服務，提供內建的高可用性與備份。

ISO/IEC 27001:2022 Requirements	Thales Solutions
應用程式安全	
8.25: 安全開發生命週期 應建立和使用軟體和系統安全開發規則。 **8.26: 應用程式安全要求** 在開發或取得應用程式時，應確定、指定和批准資訊安全要求。	CipherTrust Platform Community Edition 讓 DevSecOps 可以輕鬆地在混合和多雲應用程式中部署資料保護控制措施。 該解決方案包括 CipherTrust Manager Community Edition、資料保護閘道和 CipherTrust Transparent Encryption for Kubernetes 的授權。 CipherTrust Secrets Management 是最先進的機密管理解決方案，可保護並自動存取 DevOps 工具和雲端工作負載中的機密，包括機密、憑證、認證、API 金鑰和權杖。 CipherTrust Application Data Protection 提供開發人員友善的軟體工具，用於加密金鑰管理以及機敏資料的應用程式級加密。 它可以在資料建立或首次處理時立即進行，並且無論其資料生命週期狀態如何（在傳輸、使用、備份或複製期間）都可以保持加密狀態，以在應用程式層提供最高級別的安全性。 Thales Data Protection on Demand (DPoD) 是基於雲端的市場需求，提供 Luna HSM 和 CipherTrust 解決方案作為服務。 這使得內部團隊能夠輕鬆、安全地利用這些經過驗證和認證的資料安全解決方案，來建構他們自己的產品和服務。

關於 Thales

Thales是資料安全領域的全球領導者，深受全球各國政府和最知名企業的信賴，協助他們保護最機敏的資料。您所依賴保護您個資的企業，也依賴Thales來保護他們的資料。在資料安全方面，企業面臨越來越多的決定性時刻。無論是建置加密策略，移轉到雲端還是滿足合規性要求，您都可以依靠 Thales來確保您的數位轉型安全。