如何透過 Ekran System® 軟體遵循 SWIFT 客戶安全計劃（CSP）SWIFT CUSTOMER SECURITY PROGRAMME 法規要求

詳細的技術簡介，展示了 Ekran 系統功能如何對應到 SWIFT 客戶安全控制並展示可能的部署方案

部分代表性客戶

SWIFT 客戶安全計劃 SWIFT CUSTOMER SECURITY PROGRAMME (CSP)

為了因應不斷增長的威脅形勢，SWIFT 組織為其客戶開發並引入了正式的安全計劃。 從 2017 年 12 月開始，作為 SWIFT 用戶的任何金融機構必須遵守一套 16 項強制性安全控制措施，並採取一切合理措施來滿足 11 個諮詢安全控制措施，這些控制措施共同構成了所謂的 SWIFT 客戶安全控制框架 SWIFT Customer Security Controls Framework。每 12 個月確認一次是否合符合規範要求。

為了加強 SWIFT 客戶的網路安全並防止欺詐，該框架將行業最佳安全實踐和指南轉化為三個關鍵目標（保護您的環境、了解與限制存取、偵測與反應）。 這些主要目標在技術、組織與教育安全控制中進一步詳細說明。。.

目標 Objective	保護您的環境 Secure Your Environment	了解與限制存取 Know and Limit Access	偵測與反應 Detect and Respond
原則（和相對應的安全控制組 Security Control Groups)	1. 限制一般 IT 環境的網際網路存取並保護關鍵系統 2. 減少攻擊與和漏洞 3. 有效保護作業環境	4. 防止憑證被竊取 5. 管理身份與隔離特權	6. 偵測在系統與交易記錄中的異常活動 7.事件反應與資訊共享計劃

使用 EkranSystem® 協助您遵循 SWIFT CSP 法規要求

EkranSystem® 內部威脅防護平台是您採用 SWIFT 客戶安全控制的強大盟友。.

這種強大而靈活的基於代理程式 agent-based 的軟體支援各種 作業系統、配置與網路架構，包括 桌機、伺服器與跳板伺服器 Jump Servers。 它支援實體與虛擬基礎架構。使用 Ekran System，您可以控制對安全區域與用戶身份的存取、監控與記錄其中的任何活動，收到可疑操作的警報以及啟動事件反應。.

關鍵功能組

存取控制 Access Control

- 特權帳號與連線管理 Privileged account and session management (PASM)
- 暫時與一次性憑證密碼
- 登入時手動核可
- 整合目的驗證的票務系統 Ticketing system
- 密碼庫 Password vault

身份控制 Identity Control

- 多因子認證 Multi-factor authentication
- 登入共用帳號時二次認證以確認用戶身分

連線控測與錄影 Session Monitoring and Recording

- 視頻格式的終端機、遠端與本地連線側錄記錄索引・可搜索的多層本文索引（URL、指令、按鍵、應用程式、連接設備等）
- 可選用記錄過濾（依照用戶、應用程式或 URL）進行連續監視
- 可匯出錄影紀錄作為舉證

即時警報與事件反應 Real-time Alerting and Incident Response

- 基於模板 Template-based 與完全可自定義的針對異常、可疑與高風險事件的警報
- 提供即時警報以及相關的事件背景 •手動或自動的事件反應行動，包括警告用戶與阻止、阻斷設備(device blocking)與終止程式

詳細的安全控制– 功能對應表

Ekran System® - 一個靈活而安全的解決方案

支援平台

Windows　Mac OS　Linux　CITRIX

vmware　UNIX®

支援應用

- 應用程式強化 Application hardening
- 詳細的內部操作記錄
- 受到高度保護的資料儲存設備
- 加密的通信通道

彈性的部署

- 高可用性 High-availability 模式
- 多租戶與單租戶模式
- 與 SIEM 和票務 Ticketing 系統整合
- 用戶端自動更新，線上與離線更新
- 自我監控系統儀表板
- 易於擴展的部署

詳細的安全控制要求與 Ekransy Stem® 功能對應

安全控制 Security Control	目標 Objective	Ekran System 角色 Role
1. Restrict Access and Protect Critical Systems from General IT Environment 限制一般 IT 環境的網際網路存取並保護關鍵系統		
1.1 SWIFT Environment Protection SWIFT 環境保護	確保保護用戶的本地 SWIFT 基礎設施免受一般 IT 環境與外部環境中可能被入侵因素的影響。	Ekran System 允許安全團隊通過在安全區域內設置跳板伺服器 Jump Server 來保護 SWIFT 安全區域，並將存取服務器的權限僅限於受信任的管理員。包括密碼庫 Password Vault 內的所有相應的 Ekran System 管理元件都可以部署在安全區域內，並且可以實現認證服務隔離 Authentication Service Segregation。 通過在其上安裝 Ekran System Clients 用戶端，可以進一步保護對位於安全區域內的資源的存取，從而允許安全人員更細緻地控制用戶活動，例如通過阻止某些操作或應用程式。安裝的用戶端 Clients 提供詳細的日誌記錄與偵測能力。
1.2 Operating System Privileged Account Control 作業系統特權帳號控制	限制與控制管理員等級作業系統帳號的分配與使用。	Ekran System 提供二次身份驗證 secondary authentication 功能，根據個人憑證來識別共享帳號的真正用戶，例如內建的管理員級作業系統帳號。這不僅可以詳細記錄，還可以限制與允許特定用戶存取共用帳號。 Ekran System 提供兩種緊急存取選項，避免使用內建帳號： 一次性密碼 one-time passwords 與登錄時必須經過安全人員的強制性手動批准。使用整合驗證額外的控制目的票務系統 ticketing system，增強了啟用票證的驗證。 Ekran System 提供安全區域內啟動的每個連線詳細的深入活動監控，允許安全團隊監控所有管理員等級的活動，包括 sudo 命令和已執行腳本 scripts 的內容。
1.3 A Virtualisation Platform Protection 虛擬化平台保護	將代管到虛擬化平台與虛擬機（VM）的 SWIFT 相關元件的安全等級與實體環境相同。	Ekran System 為虛擬環境提供開箱即用的支援，為虛擬機與虛擬化平台提供完整功能。 其他功能（如整合 Golden Images 與動態授權池 Dynamic License Pools）可簡化維護。
2. Reduce Attack Surface and Vulnerabilities 減少攻擊與和漏洞		
2.1 Internal Data Flow Security 內部資料流安全	確保本地 SWIFT 相關應用程式與其與操作員 PC 的連接之間的資料流的機密性、完整性和真實性。	

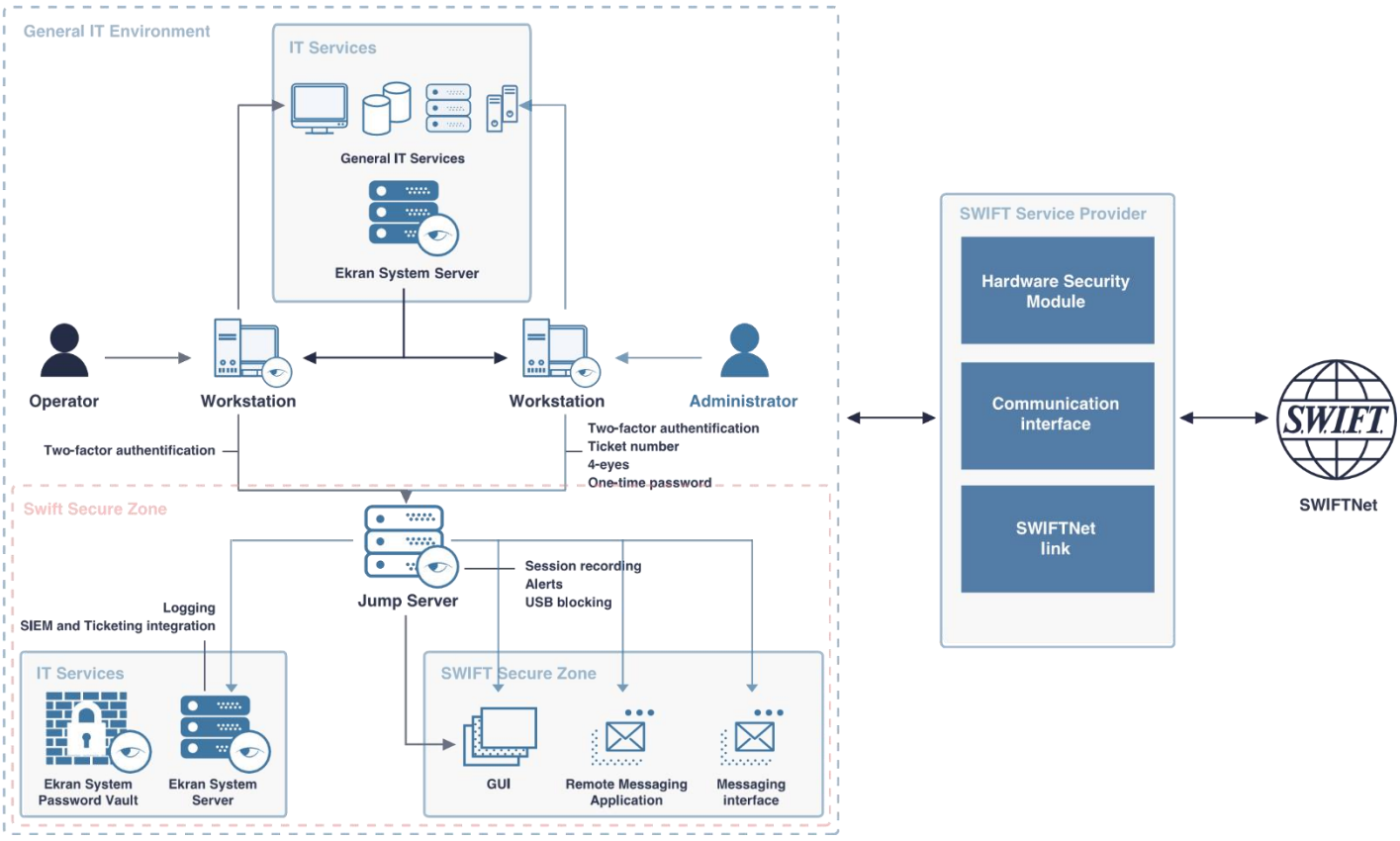
2.2 Security Updates 安全更新	應用強制軟體更新以及即時應用與評估風險相關的安全更新，確保供應商支援、最大限度地減少發生本地 SWIFT 基礎設施中已知的技術漏洞。	
2.3 System Hardening 系統強化	通過執行系統強化來減少 SWIFT 相關元件的網路攻擊面。	
2.4A Back-office Data Flow Security 後台資料流量安全	確保後台（或中介軟體 Middleware）應用程式與連接 SWIFT 基礎設施元件之間的資料流的機密性、完整性和相互認證。	
2.5A External Transmission Data Protection 外部傳輸資料保護	保護傳輸與駐留在安全區域之外的 SWIFT 相關資料的機密性。	
2.6 Operator Session Confidentiality and Integrity 連線操作保密與完整性	保護連接到本地 SWIFT 基礎設施的互動作業人員連線的機密性與完整性。	
2.7 Vulnerability Scanning 漏洞掃描	透過實施定期的漏洞掃描流程並根據結果來識別本地 SWIFT 環境中的已知漏洞。	
2.8A Critical Activity Outsourcing 外包關鍵活動	確保本地 SWIFT 基礎設施免受關鍵活動外包所帶來的風險。	Ekran System 透過其 PASM 功能無需顯示存取密碼允許安全團隊授予對安全區域的安全第三方存取權限。 所有相應的存取權限都是臨時的，可以檢查的、持續或撤消。 一次性密碼 one-time password 機制可用於提供一次性存取。 票務系統整合可以進一步驗證存取目的。 對於密切的承包商監控，可以透過安全主管的強制性手動登錄批准 manual login approval 來管制存取，並進行後續的即時視頻監控。

2.9A Transaction Business Controls 交易業務控制	將交易活動限制在經過驗證和批准的交易對手以及正常業務的預期範圍內。	
2.10A Application Hardening 應用程式強化	通過在 SWIFT 認證的訊息傳遞與通信介面與相關應用程序上執行應用程式強化，減少 SWIFT 相關元件的攻擊面。	
3. Physically Secure the Environment 有效保護作業環境		
3.1 Physical Security 有效保護	防止對敏感設備、工作場所環境、代管站點與存儲設備的未經授權的實際存取.	Ekran System 通過阻止存取或限制使用 USB 來保護伺服器免受未經授權的存取。透過設定白名單可以允許使用特定的 USB 設備，例如硬體權杖 tokens。 Ekran System 可靠地監控、警告與阻止 USB 儲存設備和任何性質的其他 USB 設備。
4. Prevent Compromise of Credentials 防止憑證被竊取		
4.1 Password Policy 密碼政策	通過實施和實施有效的密碼策略，確保密碼足以抵禦常見的密碼攻擊。	
4.2 Multi-factor Authentication 多因子認證	通過實施多因子身份驗證 Multi-Factor Authentication，防止單因子 Single Authentication Factor 身份驗證洩密允許存取 SWIFT 系統。	為了提高授權可信度，Ekran System 在登錄操作員 PC 時支援通過行動裝置 APP Mobile App 提供的基於時間的一次性密碼 time-based one-time passwords。 這為憑證被盜提供了額外的保護。
5. Manage Identities and Segregate Privileges 管理身份與隔離特權		
5.1 Logical Access Control 邏輯取存控制	實施操作員帳戶需要的存取權限、最小權限 Least Privilege 與職責分離的安全原則。	Ekran System 為特權帳號與一般用戶提供了一套廣泛的存取控制工具。 包括透過 PASM 功能在跳板伺服器 Jump Server 上進行臨時憑證管理與安全密碼庫與自動憑證配置。安全管理員為一次性存取方案產生一次性密碼。只有在安全管理員手動批准此登錄後才能存取安全端點，安全管理員可以實況監控啟動的連線。 通過與票務系統整合來驗證存取的目的。 這些工具允許安全團隊實施最佳實踐，例如職責分離 Segregation of Duties、四眼控制 Four-Eye Control，最小特權 Least Privilege 原則和基於目的的存取 purpose-based access。
5.2 Token Management 權杖管理	確保適當的管理、追踪與使用硬體身份驗證權權杖 tokens（如果使用權杖 tokens）。	
5.3A Personnel Vetting Process 人員審查處理	執行人員審查，確保操作本地 SWIFT 環境的員工的可信度。	

5.4 Physical and Logical Password Storage 實體與邏輯密碼儲存	保護實體與和邏輯記錄的密碼。	為確保密碼的安全性，Ekran System 會對其進行加密並將其儲存在密碼庫中。 用戶可以通過 Ekran System 在端點上進行身份驗證，而無需向用戶透露憑據。
6. Detect Anomalous Activity to Systems or Transaction Records 偵測在系統與交易記錄中的異常活動		
6.1 Malware Protection 惡意軟體防護	確保本地 SWIFT 基礎設施免受惡意軟體的侵害。	
6.2 Software Integrity 軟體完整性	確保 SWIFT 相關應用程式的軟體完整性。	Ekran System 軟體本身並沒有提供軟體完整性功能，但是可以選購 CIMTRAK 等 FIM 檔案完整性軟體，即時偵測軟體的完整性、防止竄改(勒索)。
6.3 Database Integrity 資料庫完整性	Ensure the integrity of the database records for the SWIFT messaging interface.	Ekran System 軟體本身並沒有提供軟體完整性功能，但是可以選購 CIMTRAK 等 FIM 檔案完整性軟體，即時偵測資料庫的完整性。
7. Plan for Incident Response and Information Sharing 事件反應與資訊共享計劃		
7.1 Cyber Incident Response Planning 網路事件反應計劃	確保採用一致有效的方法管理網路事件。	為了簡化網路事件管理，Ekran System 提供了一個集中的 UI，用於分析與反應檢測到的事件。相關事件的訊息可以自動發送到 SIEM 和/或票務系統 Ticketing System。 為了在檢測到時檢測並防止惡意或冒險活動，Ekran System 提供事件反應工具，例如自動或手動停止連線、終止應用程式、警告用戶或阻止用戶。為簡化事件管理，Ekran System 包含強大的報告和調查功能。
7.2 Security Training and Awareness 資訊安全培訓與意識	透過定期的安全培訓和宣傳活動，確保所有員工了解並履行其安全責任。	
7.3A Penetration Testing 滲透測試	通過執行滲透測試來驗證操作安全設定並發現安全漏洞。	
7.4A Scenario Risk Assessment 場景風險評估	基於合理的網路攻擊情境評估組織的風險與準備情況。	

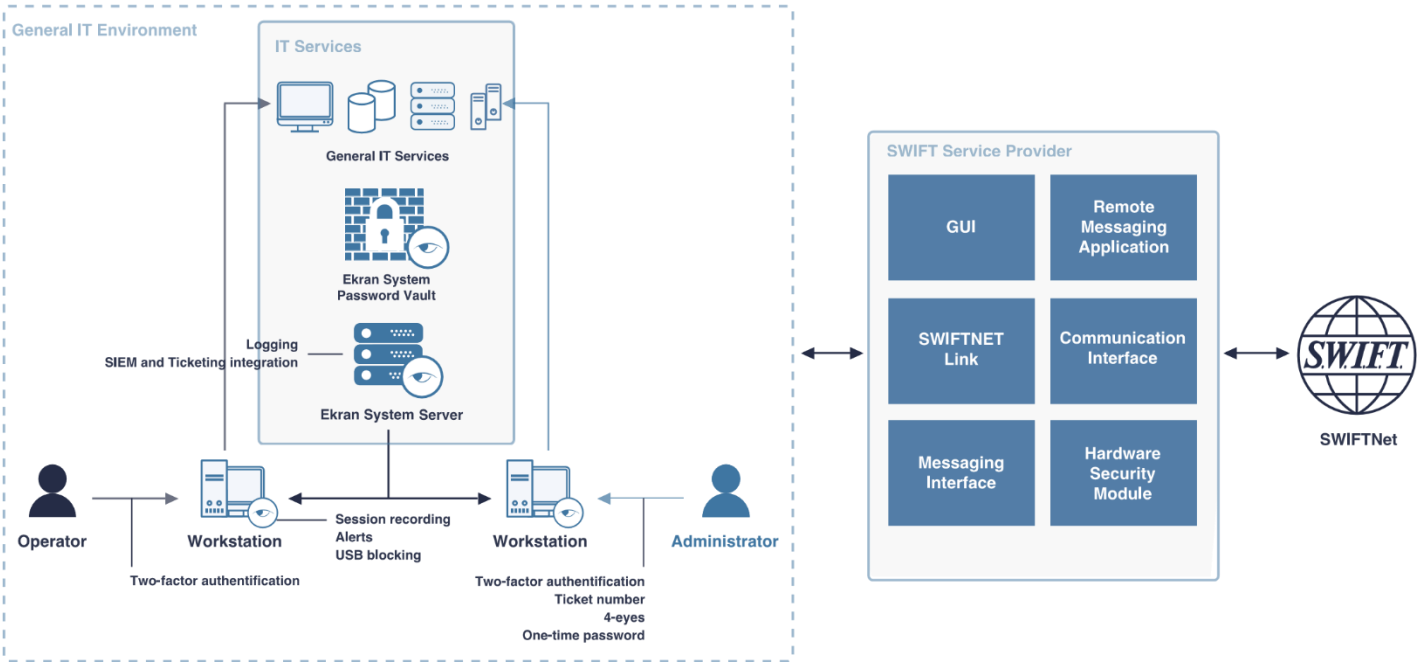
部署計劃

架構類型 A: SWIFT 基礎設施在用戶位置內



部署計劃

架構類型 B: SWIFT 基礎設施在用戶位置外



了解詳細內容

與我們聯繫

SWIFT sales: swift@ekransystem.com
Ekran System : www.ekransystem.com
商丞科技: www.proware.com.tw

www.ekransystem.com

Ekran System®