TAICS

TAICS TR-0028 v1.0:2023

5G專網服務管理系統資安評估指引

Cybersecurity assessment guidelines for 5G private network service management systems

2023 / 11 /16

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

5G 專網服務管理系統資安評估指引

Cybersecurity assessment guidelines for 5G private network service management systems

出版日期: 2023/11/16
終審日期: 2023/09/27

誌謝

本指引由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人工業技術研究院 黃維中 副所長

TC5 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC5 副主席：財團法人電信技術中心 林炫佑 副執行長

TC5 行動通訊資安工作組組長：財團法人資訊工業策進會 柯盈圳 組長

技術編輯：財團法人資訊工業策進會 王士豪、辛子睿、國立陽明交通大學 劉恩成

此指引制定之協會會員參與名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、中華電信股份有限公司、台灣是德科技股份有限公司、台灣檢驗科技股份有限公司、安立知股份有限公司、亞太電信股份有限公司、亞旭電腦股份有限公司、和碩聯合科技股份有限公司、英業達股份有限公司、神盾股份有限公司、財團法人工業技術研究院、財團法人台灣商品檢測驗證中心、財團法人資訊工業策進會、財團法人電信技術中心、啟碁科技股份有限公司、國立陽明交通大學、國立臺北大學、雲達科技股份有限公司、遠傳電信股份有限公司、德凱認證股份有限公司、緯穎科技服務股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

國立澎湖科技大學

本指引由數位發展部數位產業署支持研究制定

目錄

前言

本指引係依台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業指引。

本指引並未建議所有安全事項，使用本指引前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本指引之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

5G 專網服務管理系統是指針對 5G 專網基礎設施和服務進行遠程監控、配置和控制的管理系統。此系統負責維護 5G 網路的運行，確保網路的穩定性、功能性和安全性。儘管資安防護技術發展迅速，5G 專網的資訊安全目前偏重於個別設備為主，缺少整體服務管理系統資安防護的評估作業指引。本文即針對此部分提供資安評估流程及相關控制項檢測說明，檢測範圍涵蓋運行於 5G 專網設備上的服務管理系統，如 OAM、EMS、SMO 等服務管理系統。

112 年 6 月 1 日數位發展部發布「行動寬頻專用電信網路設置使用管理辦法」，規範網路設置計畫之應列事項，包括上線後維運管理作法，其中特別要求必須有資安偵測防護規劃；企業機構導入 5G 專網系統，除了入網前需進行個別設備安全檢測外，入網後服務管理之安全控制措施涉及維運穩定性，亦需評估全系統安全的持續有效性，以盡可能降低運營時可能遭駭的風險；因此，基於上述管理辦法及業界導入 5G 專網安全需求，同時參考美國「NIST 5G CYBERSECURITY - Preparing a Secure Evolution to 5G」安控措施建議，特擬定本評估指引提供業界參考使用。爰此，配合國家持續推動 5G 垂直整合應用，以及維繫整體資安強健體質之發展策略，針對 5G 特性資安議題，建立適用於 5G 服務管理系統之安控評估機制，提供企業機構 5G 專網資安防護評估之參考，提升其服務管理之安全性與運行之穩定性。

5G 專網場域元件包括一系列的硬體和軟體組件，通常包括核心網路元件、基地臺元件、終端設備、管理系統、及應用服務等。其中核心網路元件及基地臺元件的安全架構在 3GPP TS33.501 中定義，並在 3GPP TS33.117 提供一般安全保證要求；虛擬化相關之資安標準定義於 3GPP TS33.818 及 3GPP TS33.527。核心網路元件中網路功能的細部資安標準分別於 3GPP TS33.512 及 3GPP TS33.522 定義；基地臺元件的細部資安標準則定義於 3GPP TS33.511。管理系統的安全暨評估規範目前僅有在 O-RAN Security Tests Specifications 及 O-RAN Security Requirements Specifications 進行初步介紹，且缺乏持續性合規暨稽核的指引說明，為目前市場的缺口。本指引即為補足此缺口。5G 專網場域主要分為兩大類型：

- 企業封閉型專網(Enterprise 5G Private Network)
- 混合雲 5G 專網(Hybrid_Cloud 5G Private Network)

本指引涵蓋的安全控制項以封閉型專網安全檢測項為主，至於混合雲專網之特殊資安要求，需考量實際應用情境，擴增相對應之檢測項，唯目前尚在初步研究進行中，規劃於下一版更新時再予擴充。

依電信管理法及行動寬頻專用電信網路設置使用管理辦法之說明，一般情況下禁止 5G 專網連接公共服務網路，但緊急情況時開放連結。而，公共服務網路依行動寬頻業務管理規則之要求，於資通安全維護計畫內應載明資通安全風險評估，且為營運業者自述重點。唯公共服務網路的資安要求比 5G 專網要求高，故遭遇緊急事件需進行 5G 專網與公共服務網路連結時，應以公共服務網路的資安要求為基準。

NIST SP 800（National Institute of Standards and Technology Special Publication 800）是美國國家標準與技術研究院（NIST）所發布的一系列安全性標準和指南。當中「NIST SP 800-53」是 NIST 發布的一個安全性和隱私控制框架，旨在幫助組織確保其系統的安全性和合規性。以安全性來說，當組織部署 5G 專網時，需考慮實施適當的安全性措施，以保護 5G 網路和相關數據。而「NIST SP 800-53」提供了一個廣泛的控制列表，共定義了二十大類安全領域，298 個安全控制項供業界進行實際操作。針對 5G 網路安全特性，NIST 也提出了「NIST 5G CYBERSECURITY - Preparing a Secure Evolution to 5G」供業界參考。當中，根據「NIST SP 800-53」提出的安全控制措施，於 Security Control Map 章節，擷取出適合應用於 5G 場域的部分，共包含十大類安全領域、46 個安全控制項(Security Controls, SC)，其中包括身份認證、訪問控制、加密、安全監控等，建議組織於 5G 場域中進行實作參考。本文即採用建議之相關安全控制措施，進行服務管理系統的資安評估

本指引針對 5G 專網服務管理系統進行如下作業：(a)資產盤點暨評估檢核作業、(b)資安要求等級自評控制項核對確認作業、(c)資安防護檢測驗證作業等三道流程，並根據三道流程進行控制項驗證紀錄表實作，有效揭露應用場域是否達到基本的資訊安全防護。

1. 適用範圍

本指引定義 5G 專網服務管理系統之資安相關評估要求。5G 專網服務管理系統通常位於運營商的資訊技術中心、網路管理中心或雲端服務環境，具體的地理位置可能因不同組織的需求和佈局而有所不同。本指引適用範圍為針對已整合完成之 5G 專網場域，其中包含組合他人核心網路或接取網路。

本指引適用對象為專網服務提供商、專網設備製造商、系統整合商、軟體或硬體開發人員、系統規劃人員、服務供應商與使用者等。

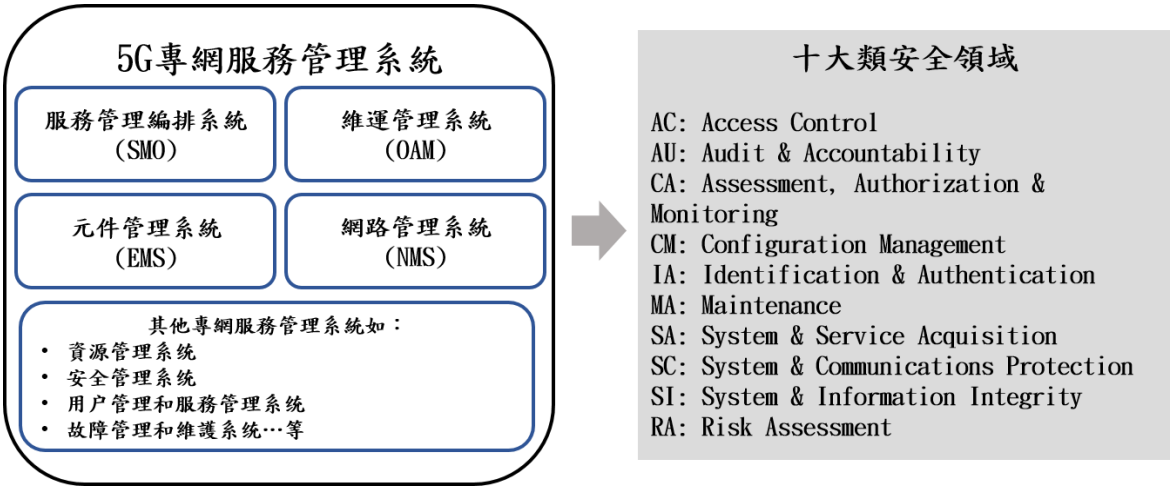

圖 1 本指引適用範圍示意圖

2. 引用標準

下列標準因本指引所引用，引用章節之內容成為本指引之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(包括補充增修)。無加註年份者，適用該最新版(包括補充增修)。

[1] 數位發展部，行動寬頻專用電信網路設置使用管理辦法，2023/06

[2] National Institute of Standards and Technology (NIST)，5G CYBERSECURITY - Preparing a Secure Evolution to 5G，2020/04

[3] National Institute of Standards and Technology (NIST)，SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations，2022/09

[4] National Institute of Standards and Technology (NIST)，SP 800-53B Control Baselines for Information Systems and Organizations，2020/10

3. 用語及定義

下列用語及定義適用於本指引。

3.1 第五代行動寬頻專用電信網路 (5G 專網, 5G Private Network, 5G PN)

參照數位發展部之「行動寬頻專用電信申請設置管理辦法」，行動寬頻專用電信網路，指設置者以所受核配之 4.8-4.9 GHz(吉赫)頻段，採用國際電信聯合會(International Telecommunication Union，簡稱 ITU)或第三代合作夥伴計畫組織(3rd Generation Partnership Project，簡稱 3GPP) 公布之第五代行動通訊技術，於核准之設置場域範圍內，設置供自己使用，且其網路架構係由核心網路、接取網路與傳輸網路所 組成之電信網路。本指引之 5G 專網定義現以數位發展部之定義為參考依據，並以政府監管單位所公告最新定義之 5G 專網為主要依據。

3.2 接取網路(Access Network, AN)

參照數位發展部之「行動寬頻專用電信申請設置管理辦法」，接取網路指透過基地臺或接取點(Access Point)發射及接收無線電訊號，將終端設備與核心網路或其他電信網路連結之網路。

3.3 核心網路(Core Network, CN)

參照數位發展部之「行動寬頻專用電信申請設置管理辦法」，核心網路指具接取管理功能（Access Management Function，簡稱 AMF）、連結管理功能（Session Management Function，簡稱 SMF）、認證伺服器功能（Authentication Server Function，簡稱 AUSF）、統一資料管理功能（Unified Data Management，簡稱 UDM）、政策控制功能（Policy Control Function，簡稱 PCF）、用戶平面功能（User Plane Function，簡稱 UPF）等之軟體或硬體元件。

3.4 基地臺(Base Station, BS)

參照數位發展部之「行動寬頻專用電信申請設置管理辦法」，基地臺指行動寬頻專用電信網路內用以傳送、接收無線電波訊號，供行動寬頻專用電信網路終端設備通信之電臺。

3.5 用戶設備 (User equipment, UE)

由通用積體電路卡(Universal integrated circuit card, UICC)和移動式設備(Mobile equipment, ME)組成，其中移動式設備可進一步由處理通訊功能的移動式終端(Mobile termination, MT)和終端設備(Terminal equipment, TE)組成。

3.6 使用者身分模組 (Subscriber Identity Module, SIM)

主要用於儲存使用者身分辨識資料、簡訊資料和電話號碼的智慧卡。

3.7 第三代合作夥伴計畫 (The 3rd Generation Partnership Project, 3GPP)

是一個成立於 1998 年 12 月的標準化機構，該機構設立的原初目的在推廣以全球行動通訊系統(Global System for Mobile communications, GSM)規格為基礎的國際行動通訊 2000(International Mobile Telecommunication-2000, IMT-2000)技術規範，提出一個能持續演進強化的國際通用技術標準規格，並於 2018 年 6 月與 2020 年 7 月正式完成 5G 獨立組網(Standalone, SA) 第 15 版本 (Release 15) 以及第 16 版本 (Release 16) 的標準制定。目前其成員包括歐洲電信標準化協會(European Telecommunications Standards Institute, ETSI)、日本無線電產業與商務協會(Association of Radio Industries and Business, ARIB)、日本電信技術委員會(Telecommunication Technology Committee, TTC)、中國通訊標準化協會(China Communications Standards Association, CCSA)、北美通訊產業解決方案聯盟(Alliance for Telecommunications Industry Solutions, ATIS)、韓國電信技術協會(Telecommunication Technical Assembly, TTA)，以及印度電信標準發展協會(Telecommunications Standards Development Society, India, TSDSI)都簽署加入這個合作性協議中。

3.8 服務管理編排系統 (Service Management and Orchestration System, SMO)

參照 O-RAN 聯盟之定義，SMO 指支持基地臺之服務管理編排系統，提供相關 5G 專用網路使用情境，如室內定位、網路切片等。SMO 根據 O-RAN 標準提供下列服務：

(a) ISO Model 之 FCAPS 功能及傳輸介面

(b) 用於基地臺優化的非即時基地臺智慧控制器(Non-RT RAN intelligence Controller, Non-RT RIC)

(c) 基於 Interfaces in O-RAN Architecture 架構，藉由 SMO 系統與雲端運算資源(O-Cloud) 介接，合作進行管理、協調和工作任務分配，或在 O-RAN 架構下通過與 O1、O2、A1、E2 等通訊介面執行服務。

(d) A1：SMO 中的非 RT RIC 和用於 RAN 優化的 RT RIC 之間的介面。

(e) O1：SMO 和 O-RAN 網路功能之間的介面，用於支持 FCAPS。

(f) 在混合模式下，SMO 和 O-RU 之間的開放式 Fronthaul M 平面介面，用於支持 FCAPS。

(g) O2：SMO 和 O-Cloud 之間的介面，提供平台資源和工作負載管理。

3.9 維運管理系統 (Operations and Maintenance System, OAM)

參照 O-RAN 聯盟之定義，OAM 指在 ISO FCAPS 管理模型下，支持故障管理 (FM)、設定管理 (CM)、權限管理(AM)、性能管理 (PM)、安全管理(SM)之模組，並以 TLS/Netconf、TR.069、Restful 介面，和其他事件處理的 HTTP 客戶端管理系統。

3.10 元件管理系統(Element Management System, EMS)

根據 O-RAN 聯盟的描述，EMS 是一個遵循 ISO FCAPS 管理模型的模組，用於處理故障管理（FM）、配置管理（CM）、權限管理（AM）、性能管理（PM）和安全管理（SM）；EMS 使用 TLS/Netconf、TR.069、Restful 介面連接 CU、DU、RU 等 5G RAN 元件進行管理，達成上述 ISO FCAPS 管理目標。

3.11 網路管理系統 (Network Management System, NMS)

網路管理系統是一種用於監控、控制和管理 5G 網路的集成平台。它是 5G 網路的重要組成部分，用於實現網路運營商對整個 5G 網路基礎設施的管理和運營。

3.12 單一專網場域 (Single PN Field)

單一專網場域包含該場域之核心網路、基地臺以及服務管理系統。其中基地臺歸屬於單一服務管理系統。

3.13 ISO FCAPS

FCAPS 是 ISO 電信管理網路模型和網路管理框架。 FCAPS 是故障、配置、審計、性能、安全（fault, configuration, accounting, performance, security）的首字母縮寫詞，是 ISO 模型定義網路管理任務的管理類別。

3.14 機密性 (Confidentiality)

機密性指的是應確保資訊的存取須經過授權。

3.15 完整性 (Integrity)

完整性指的是確保資訊的內容正確且完整。

3.16 可用性 (Availability)

可用性指的是確保經授權後的使用者，能確實存取及使用。

3.17 網路運維中心 (Network Operations Center, NOC)

NOC 負責確保企業基礎設施能夠維持業務營運以及滿足服務水平。

3.18 一次性密碼 (One-Time Password, OTP)

又稱動態密碼或單次有效密碼，是指計算機系統或其他數位裝置上只能使用一次的密碼，有效期為只有一次登錄會話或交易。一些實作還納入了雙因素認證，確保單次有效密碼需要存取一個人有的某件事物。

3.19 政府組態基準 (Government Configuration Baseline, GCB)

政府組態基準，目的在於規範資通訊設備(如個人電腦、伺服器主機及網通設備等) 的一致性安全設定(如密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之風險。

3.20 第七號發信系統 (Signaling System Number 7, SS7)

一種被廣泛應用在公共交換電話網、蜂窩通訊網路等現代通訊網路的共通頻道信號系統，是國際電信聯盟推薦首選的標準信令系統。

3.21 網路配置協議 (Network Configuration Protocol, NETCONF)

用於設定和管理網路設備的網路管理協議。它是由 IETF（Internet Engineering Task Force）制定的一個標準協議，旨在簡化網路設備的配置和管理。

3.22 CPE 廣域網管理協議/TR-069 (CPE WAN Management Protocol, CWMP)

TR069 是 CPE(Customer Premises Equipment)和 ACS(Auto Configuration Server)之間溝通的通訊協定。CPE 可以藉著這個協定完成服務開通、功能設定、檔案上傳下載、系統檢測等等初始化及營運管理的必須動作。

3.23 國際行動裝置辨識碼 (International Mobile Equipment Identity, IMEI)

用於識別行動設備的唯一識別號碼。每個行動設備都有自己獨特的 IMEI 號碼，這個號碼類似於設備的身份證號碼，可以用來追蹤和識別特定的設備。

3.24 用戶平面功能 (User Plane Function, UPF)

負責用戶設備(UE)上網連線、資料封包檢查與路由和轉發、用戶平面的流量監控與服務品質(QoS)管理、連接外部資料網路(DN)的管理、用戶平面部分策略規則管理以及合法監聽等功能。

3.25 存取與移動管理功能 (Access and Mobility Management Function, AMF)

負責用戶設備(UE)進入行動網路的註冊管理與身份驗證、非存取層(Non access stratum, NAS)信令(Signaling)的加密與完整性保護、緊急電話(Emergency call)的定位服務管理、用戶設備移動換手管理以及合法監聽(Lawful interception, LI)等功能。

3.26 連結管理功能 (Session Management Function, SMF)

負責用戶設備(UE)連結建立/修改/釋放之管理、動態主機組態協定(Dynamic Host Configuration Protocol, DHCP)功能與 IP 地址分配管理、位址解析協定(Address Resolution Protocol, ARP)代理管理、配置用戶平面功能(UPF)的流量控制、連結和服務連續性(Session and service continuity, SSC)模式、收集電信營運商收費資訊、用戶平面安全策略管理以及合法監聽等功能。

3.27 非存取層 (Non-Access Stratum, NAS)

非存取層為用戶設備(UE)與 5GC 間控制信令的機制，提供移動性管理、無線電承載(Radio bearer, RB)設定、用戶的入網與認證等網路功能。

3.28 通用漏洞揭露 (Common Vulnerabilities and Exposures, CVE)

規範於 ITU-T X.1520，係指美國國土安全部贊助之漏洞管理計畫，該計畫針對每一漏洞項目賦予其全球認可唯一共通編號。

3.29 通用漏洞評分系統 (Common Vulnerability Scoring System, CVSS)

指一套漏洞評鑑系統的判定標準，包括威脅所造成損害的嚴重性、資安脆弱性的可被利用程度與攻擊者不當運用該脆弱性的難易度，都被列入計分。自 0 分至 10 分，0 代表無風險，而 10 則代表最高風險。

3.30 跨網站指令碼攻擊 (Cross-Site Scripting, XSS)

Web 應用程式直接將來自使用者的執行請求送回瀏覽器執行，使得攻擊者可擷取使用者的 Cookie 或 Session 資料，而能假冒直接登入為合法使用者。

3.31 程式碼注入攻擊 (Code Injection)

指因行動應用程式設計缺陷而執行攻擊者所輸入之惡意指令，包括但不限於命令注入(Command Injection)及資料隱碼攻擊(SQL Injection)。

3.32 緩衝區溢位攻擊 (Buffer Overflow)

是指標對程式設計缺陷，向程式輸入緩衝區寫入使之溢位的內容，從而破壞程式執行、趁著中斷之際並取得程式乃至系統的控制權。

3.33 漏洞/弱點(Vulnerability/Weakness)

漏洞係指被公告之 CVE，弱點則是在設計或設定上不足之處，例如密碼強度不夠、開啟 telnet service 等。

3.34 加密 (Encryption)

指明文資訊透過加密數學演算法進行改變，使改變後的資料不具可讀性，而接收端用相對應的解密數學演算法可以恢復明文資訊而達到保密的目的。

3.35 通訊埠 (Port)

又稱為服務埠或連接埠，內建軟體因服務需求開啟，作為連網裝置與外部傳送/接收通訊資料。

3.36 敏感性資料 (Sensitive Data)

指洩漏時導致使用者造成損害之資料，包括但不限於個人資料、密碼、金鑰或地理位置等。此等資料依使用者行為或應用程式之運作，於裝置及其附屬儲存媒體建立、儲存或傳輸。

3.37 HTTPS (Hypertext Transfer Protocol Secure)

指利用 SSL/TLS 加密方式，提供網頁瀏覽器安全及使用者身分鑑別之加密通訊協定。

3.38 安全外殼協定 (Secure Shell Protocol, SSH)

一種加密的網路傳輸協定，可在不安全的網路中為網路服務提供安全的傳輸環境。SSH 通過在網路中建立安全隧道來實現 SSH 客戶端與伺服器之間的連線。

3.39 SSH 檔案傳輸協定 (SSH File Transfer Protocol, SFTP)

也稱安全檔案傳送協定(Secret File Transfer Protocol)，是一數據流連線，提供檔案存取、傳輸和管理功能的網路傳輸協定。

3.40 簡單網路管理協定 (Simple Network Management Protocol, SNMP)

該協定能夠支援網路管理系統，用以監測連接到網路上的裝置是否有任何引起管理上關注的情況。

3.41 多因子鑑別 (Multi-Factor Authentication, MFA)

指採用 2 種以上因子的鑑別機制，以獲得裝置之存取權限。多因子鑑別依據 4 個因子，包括所知之事(something you know)、所持之物(something you have)、所具之形(something you are)、所具之行為(something you behave)，於不同階段對同一裝置進行鑑別。

3.42 金鑰(Key)

又稱為密鑰，指為了驗證、鑑別、加密或解密之目的，而與演算法結合使用之參數。

3.43 遠端連線(Remote Connection)

提供使用者可透過網路連線的方式，在網路另一端連接到提供服務的軟體或硬體設備。

3.44 身分鑑別(User Authentication)

一種電腦存取控制之方法，允許軟體與設備用以鑑別使用者身分之機制，並可防 止未經授權之用戶存取敏感性資料之關鍵步驟。藉由通行碼、生物特徵、智慧卡...等 身分鑑別機制可用以判別使用者是否為合法使用者。

3.45 Gi-LAN（Gateway GPRS Support Node - Local IP Access Network）

在行動通訊網路中的網路節點，主要用於管理和處理數據流量。它負責將來自用戶設備的數據傳送到正確的目的地，同時也可以執行流量優化、安全性保護、服務提供等功

能，以確保高效的數據傳輸和用戶體驗。在不同的網路技術中，Gi-LAN 的角色和功能可能有所不同。

4. 服務管理系統資安評估流程

5G 專網場域包含核心網路元件、組合他人核網或接取網路、雲端運算中心、基地臺元件、終端設備、管理系統、直到最上層之應用服務等諸多元件。本指引針對 5G 專網服務管理系統進行如下三道評估作業:

(a) 資產盤點暨評估檢核作業：透過盤點專網場域資產設備，提供一「資安防護評量表」以利進行檢核作業。

(b) 資安要求等級自評控制項核對確認作業：根據不同應用場景、規模、法規要求等，進行組織安全要求自評，並選定所需之安全要求等級。此節中提供一「安全控制項分級建議表」，並於表中描述安全控制項目的說明及不同安全要求等級所建議採用的安全控制項。

(c) 資安防護檢測驗證作業：透過定義四階段查核方法進行資安檢測驗證作業。

根據上述三道流程進行控制項驗證紀錄表實作，紀錄表範例可參考附錄 A 之範本進行。

本指引透過「資安防護評量表」的產出，讓業者對場域中 5G 專網服務管理系統現況有概觀；透過「安全控制項分級建議表」中控制項的說明及安全要求分級，讓業者對控制項的內容有操作依據；最後透過「安全控制項查驗表」提供控制項的具體檢測/驗證方法，期待縮小「NIST 5G CYBERSECURITY - Preparing a Secure Evolution to 5G」中控制項於實際場域進行安全評估的落差，以利進行服務管理系統的資安評估。整體評估流程如圖 2 所示：

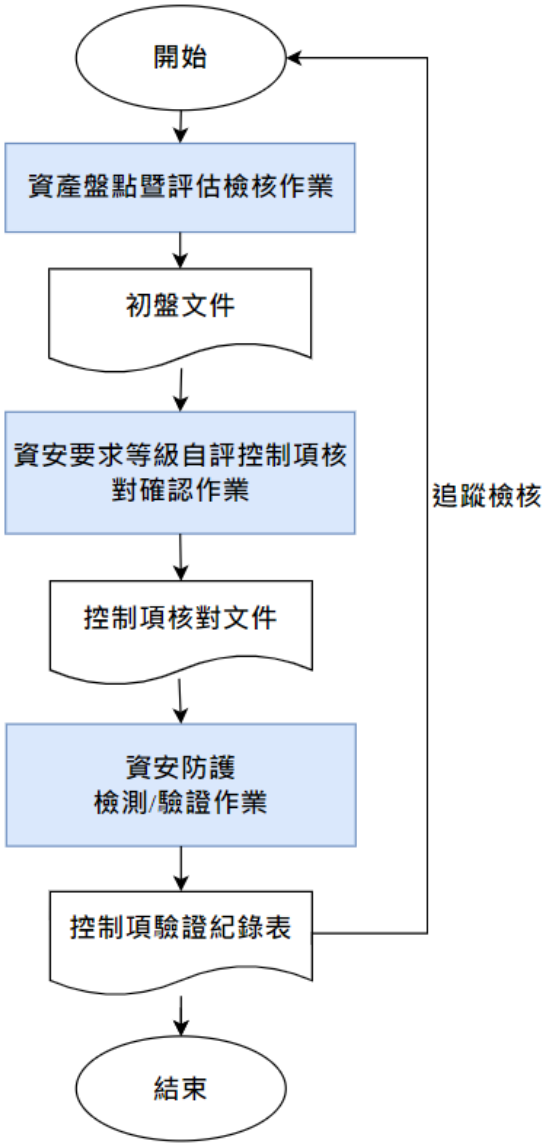

圖 2 服務管理系統資安評估流程圖

5. 資產盤點暨評估檢核作業

5G 專網是一個結合 IT、CT 及 OT 的複雜系統，整體建置需電信商、設備商、系統整合商、資訊服務商甚至雲端服務商才能共同完成。本節透過 5.1 資產盤點及建立專網場域網路架構圖方式，於 5.2 提供一資安防護評估檢核作業參考。

5.1 盤點專網場域資產設備

本作業須詳細記錄場域內所有資產設備，清楚描述各設備資訊，及須被保護的資料類型。服務管理系統需盤點的資產設備主要包含資訊資產及專網場域網路架構圖，如下描述。

5.1.1 資訊資產

5G 專網之資訊資產包含網路建設、運營和管理相關的各種數據、資訊和軟體。總體而言包含如下：

(a) 用戶資料：包括用戶的個人資訊、設備識別號碼（IMEI 等）、註冊訊息、用戶設備的特性等。

(b) 網路設備配置訊息：包括 5G 基地臺和其他網路元件的配置訊息、位置、狀態和性能監測數據等。

(c) 通訊協議和軟體：5G 網路的運作涉及多種通訊協議和軟體，包括核心網路軟體、基地臺控制軟體、安全性措施等。

(d) 運營和商業數據：包括 5G 專網場域中運營商和業務單位所涉及的數據和訊息，例如：網路流量、用戶行為、服務計費等。

(e) 安全措施：5G 專網場域中的安全措施，包括入侵檢測系統、防火牆、加密技術等。

(f) 營運和監控系統：負責監測和管理 5G 網路的運作狀態，包括網路監控、故障排除、性能優化等。

5.1.2 5G 專網場域網路架構圖

建立網路架構圖主要目的為了解系統整體運作程序，並提供後續解析場域潛在資安威脅。透過架構圖的盤點，可針對圖中界定的範圍進行相關控制項的檢核作業。如圖 3 所示：

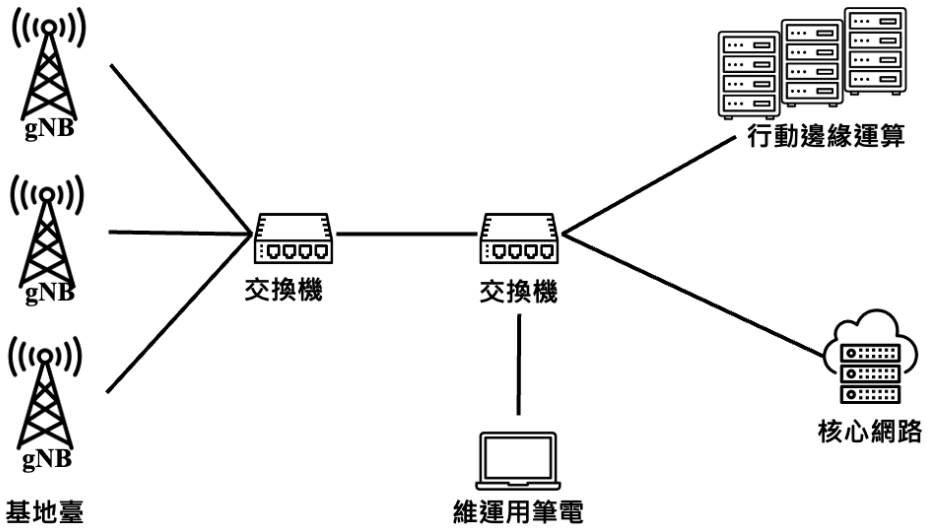

圖 3 5G 資產盤點_專網場域網路架構示意圖

5.2 專網資安評估檢核

專網場域進行資訊安全評估前，應透過場域技術/維運人員檢視須檢核的類別與項目，參考如表 1。檢核方式可透過 a.書面檢視、b.人工訪談、c.上機檢視、d.開發自動化腳本工具搜集相關跡證等方式進行。

表 1 資安防護評量表

檢核類別	檢核項目
(1) 5G 專網設備裝置與系統盤點	
(1.1) 盤點網路配置範圍	(1.1.1) 檢視 IP 地址/網段
	(1.1.2) 檢視控制平面/使用者平面/管理平面之隔離方式(Control Plane /User

	Plane /Management Plane)
	(1.1.3) 檢視流量繞送機制
(1.2) 5G 專網服務管理系統日誌	(1.2.1) 日誌是否包含：登入失敗、管理員登入、帳號管理操作、效能監控、組態變更、系統失效/重啟、網路斷線等類型之紀錄
	(1.2.2) 日誌時間是否與國際標準時間同步
	(1.2.3) 日誌是否具備防止竄改保護之機制
	(1.2.4) 日誌存錄之上限容量
	(1.2.5) 日誌存錄達上限容量後之後續處置方式
	(1.2.6) 日誌存錄是否有可歸責性（使用者/ID/Group）
	(1.2.7) 日誌存錄是否針對紀錄內容區分日誌等級
	(1.2.8) 監控機制是否可設定告警閥值
	(1.2.9) 是否有定期查核日誌的作業流程
	(1.2.10) 檢視日誌紀錄的內容格式，是否含有使用者帳號、時戳、IP 等具體可分類辨識之內容
	(1.2.11) 日誌的保留時間
(1.3) 裝置認證機制	(1.3.1) 檢視當有假基地臺與假網路元件嘗試建立連線時，能否識別真偽
	(1.3.2) 檢視現有裝置的身分識別機制為何，如：基地臺、AMF 等網路元件
	(1.3.3) 如設備規格有硬體信任根(Root of Trust)，是否有使用此功能或開啟此功能
(2) 5G 專網軟體與系統漏洞管理機制	
(2.1) 風險評估	(2.1.1) 確認是否執行風險評估機制 - 若有執行的風險評估機制，即執行

	(2.1.2) 之評估項目
	(2.1.2) 檢視是否有內部專責單位或委外負責進行專網場域風險評估
	(2.1.3) OAM 系統是否規劃備援流程與執行備援之機制
	(2.1.4) 風險評估頻率為何
	(2.1.5) 風險評估項目，是否包含客戶隱私風險評估
	(2.1.6) 風險評估項目，是否包含供應鏈安全管理
	(2.1.7) 是否針對離職員工或人員異動時，進行帳號鎖定或密碼更換
(2.2) 弱點掃描	(2.2.1) 檢視是否有進行弱點掃描 - 若有執行弱點掃描，即進行(2.2.2) 評估項目
	(2.2.2) 檢視執行弱點掃描頻率
	(2.2.3) 檢視弱點掃描係針對哪一個平面(Control Plane /User Plane /Management Plane)來執行
(2.3) OAM 系統監控	(2.3.1) 檢視 OAM 監控範圍包含哪些網元
	(2.3.2) 檢視是否有對非法 SIM 卡進行監控
	(2.3.3) 檢視是否有監控專網場域部署之防火牆的日誌
	(2.3.4) 檢視是否有監控跳板機的日誌
(3) 5G 專網軟體備份與復原機制	
(3.1) 備份資料之保護	(3.1.1) 檢視 5G 專網設備與軟體盤點範圍與盤點資料種類
	(3.1.2) 備份資料的範圍包含哪些元件
	(3.1.3) 檢視是否包含基地臺與核網的組態與用戶資料
	(3.1.4) 檢視通聯紀錄是否會進行備份
	(3.1.5) 檢視如何保護使用者隱私。如：通聯紀錄
	(3.1.6) 是否有進行備份還原的環境與機制
	(3.1.7) 是否有進行備份還原演練
(4) 5G 專網軟體安全更新機制	
(4.1) 漏洞修補	(4.1.1) 檢視是否制定軟體安全更新流程
	(4.1.2) 檢視是否有機制確保供應商與第三

	方廠商，在發生重大資安風險時主動通知
	(4.1.3) 檢視是否有定期確認裝置存在漏洞的機制
	(4.1.4) 檢視是否制定緊急軟體漏洞修補更新流程
(4.2) 完整性驗證	(4.2.1) 檢視更新流程是否包含軟體完整性驗證流程
	(4.2.2) 檢視更新流程是否包含底層的基礎網路設備。如：Switch、Router 等
	(4.2.3) 檢視核網虛擬機/容器之備份的映像檔，是否有完整性驗證
	(4.2.4) 檢視完整性驗證是否包含 OAM 系統軟體本身
(5) 5G 專網管理層是否採用 HTTPS、SSH、SFTP 及 SNMPv3 之安全協議	
(5.1) 管理層使用通訊協議	(5.1.1) 核網、基地臺、OAM、底層傳輸設備的管理層，是否使用安全協議
	(5.1.2) OAM 跟核網是否使用安全協議
(6) 5G 專網遠端維運通道保護機制	
(6.1) 維運控制措施	(6.1.1) 檢視專網上線後是否關閉遠端維運通道
	(6.1.2) 檢視連入 5G 核網之 SSH 協議是否有白名單 IP 機制
	(6.1.3) 檢視遠端管理的保護機制為何。如：身分驗證機制、授權、可歸責性
	(6.1.4) 檢視拋送至網路運維中心(NOC)之資料，其資料傳輸的保護機制為何
(7) 5G 專網之維運管理通道與企業內網/網際網路/雲端服務間應設置防護設備或機制	
(7.1) 網路分隔或封包過濾機制	(7.1.1) 檢視有無防火牆或類似技術
	(7.1.2) 檢視有無網路分隔
	(7.1.3) 檢視控制平面(Control Plane)與使用者平面(User Plane)是否在同一個子網(Subnet)下
	(7.1.4) OAM 系統是否運行於獨立子網(Subnet)
	(7.1.5) 邊界防護機制為何。如：與第七號發信系統 SS7 的介面、與網際網路的介面
(8) 通道應採用專線或採用虛擬私人網路配合強健的身分辨識與授權機制	
(8.1) 遠端通道的身分辨識機制	(8.1.1) 檢視是否採用多因子認證機制
	(8.1.2) 檢視維運用跳板機是否有使用專線

	(8.1.3) 如何實作身分辨識機制 - 設定在防火牆的 VPN 上或一次性密碼(OTP)
(9) 專網白名單管理機制	
(9.1) 白名單管控	(9.1.1) 檢視是否使用帳號白名單，限制遠端連線目的地。如：僅限 OAM、NMS 或維運跳板機等
	(9.1.2) 是否有允許特定時間連入的白名單。如：週一至週五得連入
(10) 檢視連結遠端維運通道之設備(例如：終端電腦與維運用跳板機)	
(10.1) 檢視跳板主機或管理介面所用的維運主機安全要求	(10.1.1) 檢視作業系統是否具備強固性要求設定。如：政府組態設定(GCB)
	(10.1.2) 確認是否部署可防範端點惡意程式之軟體
	(10.1.3) 檢視應用程式白名單是否存在於端點設備
	(10.1.4) 檢視事件日誌記錄管理，是否採用符合業界實務做法，並定期審核紀錄
(11) 是否提供具符合業界實務之管理平面(Management Plane)帳戶管理機制	
(11.1) 帳戶管理機制	(11.1.1) 檢視存取控制的政策
	(11.1.2) 確認是否有特定維護帳號的登入日誌。如：Admin、Auditor
	(11.1.3) 檢視操作人員的身分辨識機制為何
(12) 確認是否載明空中介面(Air interface)所支援之 3GPP 安全協議	
(12.1) 密碼學的保護範圍	(12.1.1) 檢視採用何種加密演算法
	(12.1.2) 檢視基地臺到核網、核網元件之間、核網到 Gi-LAN、Gi-LAN 到網際網路出口，這中間的通道是否採用加密機制
	(12.1.3) 檢視確認 5G 系統的加密機制正常運作

6. 資安要求等級自評控制項核對確認作業

5G 專網服務管理系統的資安防護與傳統 IT 領域針對單一系統不同，其牽涉多樣的設備與相異技術架構，因此為確保專網達到一定的資安防護能力，本節依據「NIST 5G CYBERSECURITY - Preparing a Secure Evolution to 5G」為基礎，引用參照「NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations」，詳列十大類安全領域、46 個安全控制項(Security Controls, SC)，透過實施這些安全控制項，確保系統和數據在潛在的威脅下能保持安全和可靠。

5G 專網場域根據不同應用場景、規模、法規要求等，有不同程度的風險及安全需求，本節依據「NIST SP 800-53B Control Baselines for Information Systems and Organizations」為基準，評估專網系統對組織運營的重要性和價值、及可能遭受的損失程度，將安全要求等級分為低、中、高，並提供相應之安全控制項分級建議表。不同安全要求等級所建議執行的安全控制項的項目數有所不同，以確保在不同應用場景及垂直領域，建立適當之資安防護，提高整體 5G 專網安全性，保障系統面對各種安全威脅及風險之防護。

6.1 5G 專網資通安全要求等級

5G 專網資通安全要求等級定義依據「NIST SP 800-53B Control Baselines for Information Systems and Organizations」為基礎，由組織根據業務需求、特定部門要求、操作環境、個人隱私及利益、行政命令、法規、法律、政策或行業最佳實踐等因素，評估場域的風險，並根據專網場域對於組織營運的重要性和影響進行自我評估，並擇定安全要求的級別。

6.2 5G 專網系統建議之資安控制項

本節將安全要求等級分級分成低、中、高三個等級，提供明確安全建議要求與檢視方向。業者先進行安全要求等級自評，接著根據場域現狀進行 6.2 控制項的核對確認。控制項核對確認為確保該控制項可在目的場域中進行實際的檢測及驗證。參考如表 2：

表 2 安全控制項分級建議表

項目代號	安全控制項目	安全要求分級			NIST SP 800-53 參考對應
		低	中	高	
Access Control (AC)					
SC01	- 電信系統之核心網路(5G Core Network)元件應具備合適的訪問控制策略機制，並於核心網路的管理介面進行實作，僅能執行已經授權的存取，並有效保護訊息跟系統資源，包含訪問控制的策略(policies)、公司帳號群組應具備設置文件、設備帳號應有群組清單、帳號應歸屬分類等。	V	V	V	AC-3 Access Enforcement
SC02	- 電信系統之核心網路(5G Core Network)元件應根據受稽核單位所定義的訊息控制策略進行實作，並執行已批准的授權，以控制系統內和連接系統之間的訊息通道。		V	V	AC-4 Information Flow Enforcement
SC03	- 電信系統之核心網路(5G Core Network)元件之維運通道與企業內網/公共電信網路/網際網路間應設置遠端維運通道，並為此通道建立和記錄使用限制、配置/連接要求和實施指南。 - 通道採用專線或採用虛擬私人網路配合強健的身分辨識與授權機制，如多因子認證、白名單管控，限制遠端連線目的地(dst.)，如僅限 OAM (Operations, Administration and Maintenance) 、NMS 或者跳板機等。 - 用於連結遠端維運通道之設備（如：終端電腦與跳板機）應具強固性要求設定（如: GCB），並安裝防範端點惡意程式之軟體。 - 事件日誌記錄管理應採用符合業界實務做法並定期審核紀錄。	V	V	V	AC-17 Remote Access
SC04	- 電信系統之核心網路(5G Core Network)元件之運營/維護策略需要一致，並針對個人或單位從外部系統訪問系統、使用外部系統處理、存儲或傳輸組織控制的訊息進行有效的管理。	V	V	V	AC-20 Use Of External Information Systems
Audit and Accountability (AU)					
SC05	- 5G 網路部署的政策和與程序都需要有相應的狀態紀錄，包含所所有重要狀態轉換事件都應該記錄在日誌中。任何來自維運、	V	V	V	AU-2 Audit Event

項目代號	安全控制項目	安全要求分級			NIST SP 800-53 參考對應
		低	中	高	
	操作、控制的日誌都應該可以被評估並且通過系統日誌。				
SC06	- 需要評估的 5G 核心網路維運及控制日誌的內容應該要確保其完整性，所紀錄日誌的內容應包括所有適當的上下文，以便評估者能夠判定事件發生的時間/執行內容/執行者。	V	V	V	AU-3 Content of Audit Records
SC07	- 5G 核心網路的評估日誌應確保其儲存容量足夠，提供足夠的評估日誌存儲容量與監控機制十分重要。 - 在評估日誌的硬體設施或相關的軟體系統中，應有針對評估日誌的儲存容量進行監控跟警示的機制。	V	V	V	AU-4 Audit Storage Capacity
SC08	- 5G 核心網路的日誌系統於稽核處理失效(如儲存容量不足)之情況下，具有針對該事件監控回報之機制。組織可以選擇根據故障類型、故障位置、故障嚴重性等因素的組合來定義記錄過程故障的附加操作，方能即時對應。	V	V	V	AU-5 Response to Audit Processing Failures
SC09	- 5G 專網場域的管理者必須定義適當的政策與機制去進行定期的內部評估程序，並且定義不適當或著異常活動的定義，以及定義相關負責的人員或角色。	V	V	V	AU-6 Audit Review, Analysis, and Reporting
SC10	- 5G 專網場域的評估與維運系統應盡可能地簡化評估流程複雜度以及報告生成的自動化，以及日誌或報告的 API，並可做為事後調查。		V	V	AU-7Audit Reduction and Report Generation
SC11	- 5G 評估日誌的時間標記應該要有辦法進行同步和周期性更新，確保相關日誌的生成時間戳記(TimeStamp)是有意義的，相關時間戳記應可以對照映射到協調世界時 (UTC) 或格林威治標準時間 (GMT)，並根據需要決定相應的精度。	V	V	V	AU-8 Time Stamps
SC12	- 在 5G 核心網路的操作系統中，前述進行評估與維運系統的使用者權限應確保不被未經授權的連線進行登入、修改或刪除。	V	V	V	AU-9 Protection of Audit Information
SC13	- 在 5G 核心網路的操作系統中，面對使用者的任何操作，其操作記錄應具備不可否認性，如輸入、傳送或接收指令/文件，針對特定權限進行批准、更新或修改等。			V	AU-10 Non-Repudiation

項目代號	安全控制項目	安全要求分級			NIST SP 800-53 參考對應
		低	中	高	
SC14	- 所有儲存在 5G 核心網路的評估、操作或根據場域需求所保存下來的日誌或記錄文件檔案等，應根據場域政策保存相關訊息，並根據安全事件等事後調查需求提供協助，以滿足監管和組織訊息保留要求，直到確認不再需要相關資訊用於管理、法律、評估或其他操作目的。	V	V	V	AU-11 Audit Record Retention
SC15	- 根據場域或公司政策所記錄的 5G 操作或任何事件，應根據評估需求從所有事件中產生相對應的評估紀錄或評估檔案的能力。 - 評估紀錄可以由不同的事件或著是元件、日誌等產生，這些事件通常經由場域或公司政策制定哪些訊息需要被紀錄。	V	V	V	AU-12 Audit Generation
Security Assessment and Authorization (CA)					
SC16	- 在對 5G 場域設備進行管理時，場域管理者應有持續監控場域設備之能力與相應的授權管理操作系統。 - 應具備設定監控頻率、持續安全監控策略、監控與安全機制之對應機制，並對監控事件結果設置警示機制。	V	V	V	CA-7 Continuous Monitoring
Configuration Management (CM)					
SC17	- 進行 5G 核心網路的參數管理時，維運管理者應確定 5G 管理系統參數變更方式；針對參數的變更進行權限控制，並訂定批准變更之機制。 - 應提出變更權限控制與造成的安全影響分析。 - 針對所有變更參數的決策應進行紀錄，並根據場域需求保留一定時間；前述變更的記錄應定期進行評估，並周期性地進行討論確保上述機制與時俱進。		V	V	CM-3 Configuration Change Control
SC18	- 進行 5G 核心網路的參數管理時，應在變更參數前確認安全影響分析，確認其潛在安全影響。	V	V	V	CM-4 Security Impact Analysis
SC19	- 進行 5G 核心網路的參數管理時，應建立並定時更新所有系統之元件清單，確保其系統的授權範圍；針對參數管理有關的系統元件清單，應定時評估並更新。	V	V	V	CM-8 Information System Component Inventory
SC20	- 進行 5G 核心網路的參數管理時，應確認針對管理人員的角色、職責以及權限配置		V	V	CM-9 Configuration

項目代號	安全控制項目	安全要求分級			NIST SP 800-53 參考對應
		低	中	高	
	管理流程，確保系統在開發或維運周期中，相對應的人員及參數管理的權責分明，並保護參數管理機制不會被未經授權的人員揭露、修改或刪除。				Management Plan
SC21	- 進行 5G 核心網路的參數管理時，需確保場域或相關的設備符合契約內容，應保留相關授權、版權或軟體使用許可的相關憑證或文件。所有文件應建立追蹤機制，確保其複製及分發的過程受到控制，並確認參數管理範圍內的系統不會使用到未經授權或受到版權保護的內容或設備。	V	V	V	CM-10 Software Usage Restrictions
Identification and Authentication (IA)					
SC22	- 操作 5G 場域設備或系統時，應確保系統可唯一地識別和驗證組織用戶。	V	V	V	IA-2 Identification and Authentication Organizational Users
SC23	- 操作 5G 場域設備或系統時，應確保系統可唯一地識別和驗證可進行連線的設備。		V	V	IA-3 Device Identification and Authentication
SC24	- 操作 5G 場域設備或系統時，應確保系統用戶的權限、更新等機制正常運作，並確保未經授權的用戶無法進行權限外的運作。	V	V	V	IA-4 Identifier Management
SC25	- 操作 5G 場域設備或系統時，應確保有建立和實施初始身份的流程、忘記用戶密碼的恢復機制或撤銷用戶身份的管理程式。	V	V	V	IA-5 Authenticator Management
SC26	- 操作 5G 場域設備或系統時，系統對密碼的管理及驗證機制，應確保符合當地法律、行政命令、指令、政策、法規、標準和此類密碼驗證指南的要求。	V	V	V	IA-7 Cryptographic Module Authentication
Maintenance (MA)					
SC27	- 在進行 5G 場域維運行動時，應以書面或工具記錄組織維運人員、處理目的、範圍、角色、職責、維運目標、不同組織間的權責分配及相應系統維護政策，並確保這些政策及記錄有周期性地更新並稽核。	V	V	V	MA-2 Controlled Maintenance
SC28	- 在進行 5G 場域維運行動時，應定義組織維運工具。		V	V	MA-3 Maintenance Tools

項目代號	安全控制項目	安全要求分級			NIST SP 800-53 參考對應
		低	中	高	
	- 應持續的管理及監控定義之維運工具，並確保這些政策及記錄有周期性地更新並評估。				
SC29	- 在進行 5G 場域遠端維運行動時，應有特定的流程去審核、批准及監控遠端維護、保養或檢查行動，並僅允許在場域或企業規劃中的維運工具。在建立連線時採用強驗證機制並持續監控，並有明確的檢查終止或完成連線的機制或流程。	V	V	V	MA-4 Nonlocal Maintenance
SC30	- 執行 5G 場域遠端維運行動時，應建立維修人員授權流程與維護授權維修機構或人員名單。 - 需確保對系統進行維護的非陪同人員也具有所需的訪問權限。 - 指定具有所需訪問權限和技術能力的組織人員來監督不具備所需訪問權限的人員的維護活動。	V	V	V	MA-5 Maintenance Personnel
SC31	- 在 5G 系統發生故障時，應在場域或營運方定義的時間內得到維修的行動及相應的零組件。		V	V	MA-6 Timely Maintenance
Risk Assessment (RA)					
SC32	- 針對管理的 5G 場域及系統，應對系統及其處理、儲存或傳輸的訊息進行未經授權的訪問、使用、揭露、中斷、修改或破壞的風險評估，包括風險的發生機率以及衝擊程度。 - 並將風險評估結果記錄在風險評估報告；確認過後的風險評估結果應周期性的更新，並確保更新的時候讓所有相關的人員知道其更新內容、操作環境發生重大變化（包括識別新威脅和漏洞），或其他可能影響系統安全狀態的條件。	V	V	V	RA-3 Risk Assessment
SC33	- 針對管理的 5G 場域及系統，應對系統進行弱點掃描，並周期性的確認掃描結果，以及識別和報告可能影響系統/應用程序的新漏洞。 - 採用漏洞掃描工具和技術應妥善記錄，並確保管理過程。 - 根據企業組織的風險評估程序修復漏洞並與相關人員共享從漏洞掃描過程和安全控	V	V	V	RA-5 Vulnerability Scanning

項目代號	安全控制項目	安全要求分級			NIST SP 800-53 參考對應
		低	中	高	
	制評估中獲得的訊息，以幫助消除其他系統中的類似漏洞。				
System and Services Acquisition (SA)					
SC34	- 整個 5G 系統的訊息、元件或產品提供一定程度的保護，並實施有竄改保護機制，避免系統遭受逆向工程、修改和替換。			V	SA-18 Tamper Resistance and Detection
System and Communications Protection (SC)					
SC35	- 5G 系統的用戶層與管理層應該要分開（包含提供給用戶的服務）。用戶層與管理層的分離可以是實體分離或邏輯上的。如使用不同的元件、不同的 CPU、不同的 OS、不同的 IP、VNF 或其他方法的組合來實現系統管理層與用戶層的分離。		V	V	SC-2 Application Partitioning
SC36	- 5G 系統的安全功能與非安全功能應該要分開。 - 安全功能與非安全功能的分離可以是實體分離或邏輯上的。如使用不同的元件、不同的處理器模式、不同的加密權限或其他方法的組合來實現系統管理層與用戶層的分離。			V	SC-3 Security Function Isolation
SC37	- 在 5G 場域的邊界，應該監視與控制連接系統內部與外部的通訊，並在實體上或邏輯上達成網路分離，並根據場域要求，由特定的安全保護設備（如防火牆）提供連接到外部網路或訊息系統。	V	V	V	SC-7 Boundary Protection
SC38	- 於 5G 場域內進行相關訊息傳輸的時候，應該要確保其傳輸的機密性或完整性。		V	V	SC-8 Transmission Confidentiality and Integrity
SC39	- 5G 場域中應具備根據場域方要求的密碼建立、管理及密鑰的建立及管理機制。可以使用手動程序或具有支持手動程序的自動機制來執行加密密鑰管理和建立。	V	V	V	SC-12 Cryptographic Key Establishment and Management
SC40	- 5G 管理系統中的密碼強度及演算法機制應該要符合當地法規。	V	V	V	SC-13 Cryptographic Protection
SC41	- 5G 管理系統的遠端連線應具備完整的保護，並建立完善的流程機制包含監控、紀錄、警報等機制。	V	V	V	SC-15 Collaborative Computing Devices

項目代號	安全控制項目	安全要求分級			NIST SP 800-53 參考對應
		低	中	高	
SC42	- 5G 管理系統與元件間傳輸的訊息交換應該要具備明確的對應關係。				SC-16 Transmission of Security Attributes
SC43	- 5G 管理系統及周邊元件的的資料儲存應該具備加密及加密管理的機制，確保其完整性。保護的系統訊息包含與防火牆、路由器、入侵檢測、預防系統、身份驗證機制等參數或訊息。		V	V	SC-28 Protection of Information at Rest
System and Information Integrity (SI)					
SC44	- 5G 管理系統應具備檢查、回報與更正系統缺陷的能力，並在安裝更新前確認其軟體及硬體更新的有效性及限制，並有完善的更新檢查機制。	V	V	V	SI-2 Flaw Remediation
SC45	- 5G 管理系統應具備訊息監控能力，檢查未經授權的連接、並有效部署監控設備；保護入侵監控工具的訊息避免遭未經授權的修改或刪除，並確保符合 5G 相關資安檢測流程及要求等。	V	V	V	SI-4 Information System Monitoring
SC46	- 5G 管理系統應確認其軟體、硬體跟訊息的完整性，並能監控未經授權的修改。		V	V	SI-7 Software, Firmware, and Information Integrity

7. 資安防護檢測驗證作業

本節定義四階段查核方法進行資安檢測驗證作業。四階段查核方法分別為：弱點檢測、服務埠掃描、資料傳輸加密檢測、安全控制項驗證。透過四階段查核，檢測驗證專網設備與服務管理系統是否存在資安風險，作為後續產製資安稽核報告之內容佐證。

7.1 5G 專網設備及服務管理系統弱點檢測

5G 專網系統資安防護檢測驗證第一階段，使用系統/網站弱點掃描等功能之工具，對專網設備進行弱點掃描，評估是否存在 CVE 漏洞，且掃描結果應不可存在 CVSS 評等為重大風險 (Critical Level) 與高風險 (High Level) 等級之公開漏洞，若服務管理系統具備網頁 UI 介面則不可存在 Injection、XSS 及 Buffer Overflow 等常見之資安攻擊危害。掃描工具可參考附錄 B 之弱點掃描工具。

7.2 5G 專網環境連接埠掃描

5G 專網系統資安防護檢測驗證第二階段，使用網路服務埠之掃描工具，驗證專網設備是否存在預期以外的服務埠，掃描工具可參考附錄 B 之連接埠掃描工具。

7.3 5G 資料傳輸加密檢測

5G 專網系統資安防護檢測驗證第三階段，使用安全通道檢測工具或側錄網路封包工具，檢測是否採用安全傳輸通道，以確保專網資料傳輸時之機密性與完整性，檢測工具可參考附錄 B 之傳輸加密檢測工具。

7.4 5G 專網系統資安控制項驗證

5G 專網系統資安防護檢測驗證第四階段，依據第六節資安要求等級自評控制項核對確認作業後，選出於場域運行檢測的控制項，此時可針對建議實作的控制項、配合表 3 進行檢測/驗證作業。相關作業可透過 (a)書面檢視、(b)人工訪談、(c)上機檢視、(d)開發自動化

腳本工具搜集相關跡證等方式進行，確保專網達到安全控制項要求。安全控制項檢測及驗證方式、與表 1 資安防護評量表項目對應，如下表 3 所示：

表 3 安全控制項查驗表

項目代號	檢測/驗證方法	表 1 資安防護評量表對應
Access Control (AC)		
SC01	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 登入專網設備之指令介面並以指令查詢之後，應至少可查證存在兩個以上的使用者帳戶 - 登入專網設備之指令介面並查詢登入紀錄，比對使用者、維運人員有無根據不同的身分 Group 進行登入操作	11.1.1 11.1.2
SC02	- 登入專網設備之指令介面並以指令查詢之後，調查有無紀錄已批准的授權策略及規則，以及對應的網路拓墣對應機制，並做好網路區隔驗證有無根據不同的策略執行已批准的授權 - 蒐集專網設備介面與連接系統之管理介面封包之後，比對封包實際傳輸之策略與規則與批准的授權策略及規則是否一致	1.1.1 1.1.3
SC03	- 登入專網設備指令介面並以指令查詢，確認有無發現相關設定或紀錄 - 以維運人員提交場域規劃文件為基礎，檢查實受評估之專網環境與硬體拓墣之後，調查有無專屬的硬體獨立之維護通道被建立出來，與配置/連接要求和實施指南是否一致	8.1 9.1 10.1
SC04	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	3.1.1
Audit and Accountability (AU)		
SC05	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 登入專網設備指令介面並以指令查詢，確認有無系統日誌紀錄設備相關操作控制紀錄	1.2.1
SC06	- 維運人員應提出相關設備規格書面文件	1.2.10

項目代號	檢測/驗證方法	表 1 資安防護評量表對應
	- 登入專網設備指令介面並以指令查詢，確認日誌紀錄內容是否辨識事件發生之時間/執行內容/執行者	
SC07	- 維運人員應提出相關設備規格書面文件 - 登入專網設備之系統並以指令確認稽核日誌的所在位置之後，並確認有無建立以硬體與軟體有關的系統容量監控或告警機制	1.2.4
SC08	- 維運人員應提出相關設備規格書面文件 - 從維運人員提供相關佐證資料確認有無部署 OAM 協助持續監控	1.2.5 1.2.8
SC09	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	1.2.9
SC10	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 登入專網設備之系統介面並以指令確認稽核日誌的紀錄方式後，驗證對其報告或日誌具有相應的 API 機制	
SC11	- 可登入專網設備之系統並以指令確認稽核日誌的系統的時間更新機制，並實際與有更新的稽核用電腦進行比對	1.2.2
SC12	- 維運人員應提出相關設備規格書面文件 - 稽核者登入專網設備系統並確認帳號密碼管理機制是否有效，並檢查有無刪除跟修改	1.2.3
SC13	- 維運人員應提出相關設備規格書面文件 - 登入專網設備之系統並以程式指令與人工檢視調查稽核日誌之紀錄方式及相應保護機制，並透過測試工具確認其報告或日誌具有不可否認性的保護機制 - 以自動化工具嘗試篡改稽核日誌紀錄，若無法修改，則確認了對其報告或日誌具有不可否認性的保護機制	1.2.6
SC14	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 上機登入受評估之專網設備手動查詢	1.2.11

項目代號	檢測/驗證方法	表 1 資安防護評量表對應
SC15	- 登入專網設備系統並以指令確認稽核日誌的紀錄方式及產生方式後，確認其日誌運作的時間以及有無針對內容進行紀錄	1.2.1 1.2.10 2.3.3 2.3.4
Security Assessment and Authorization (CA)		
SC16	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 稽核者登入專網設備系統並以指令確認稽核日誌的蒐集及監控機制，確認其日誌的蒐集紀錄機制正常運作 - 從維運人員提供相關佐證資料確認有無部署 OAM 協助持續監控	2.3
Configuration Management (CM)		
SC17	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	
SC18	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	
SC19	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	
SC20	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 以多種不同權限之帳號登入專網設備系統，嘗試操作非帳號授權目的之操作行為，確認是否受到管制	11.1.1
SC21	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	10.1.3
Identification and Authentication (IA)		
SC22	- 檢查系統的登入機制以及用戶驗證流程的檢查，確認其系統登入程序為使用帳號密碼進行登入	11.1.3
SC23	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 從維運人員提供相關佐證資料確認有無部署 OAM 協助持續監控管理專網設備	6.1.2

項目代號	檢測/驗證方法	表 1 資安防護評量表對應
SC24	- 檢查專網設備管理系統的用戶權限管理機制，確認其系統用戶管理可根據不同的權限進行群組設定、更新	11.1.1
SC25	- 檢查專網設備管理系統的用戶權限管理機制，確認其系統用戶管理有相應流程進行建立或刪除機制	12.1.3
SC26	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	12.1.1
Maintenance (MA)		
SC27	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 稽核者將書面文件佐證之資訊與專網系統帳號之日誌與權限進行比對，對應人員及權限關係是否吻合	11.1.1
SC28	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	
SC29	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	6.1.1 6.1.3
SC30	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	
SC31	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	
Risk Assessment (RA)		
SC32	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	2.1
SC33	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 應出具專網設備弱點掃描報告作為佐證資料	2.2 4.1.3
System and Services Acquisition (SA)		
SC34	- 維運人員應提出設備規格書面文件 - 稽核者登入專網設備系統並以指令確認稽核日誌的紀錄方式及產生方式後，嘗試以腳本指令篡改日誌內容，驗證是否具備防篡改機制	1.3
System and Communications Protection (SC)		

項目代號	檢測/驗證方法	表 1 資安防護評量表對應
SC35	- 維運人員應提出設備規格書面文件 - 稽核者登入核心網路系統並確認使用應用程式的普通用戶無法訪問 管理界面，這些界面預計在單獨的（不可路由的）網路/vLAN 上運行	1.1.2 7.1.3 7.1.4
SC36	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	
SC37	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	7.1.1 7.1.2 7.1.5
SC38	- 經稽核者部署安全通道檢測工具或側錄網路封包之工具搜集封包資訊，確認其通訊傳輸是否採取安全傳輸通道進行傳輸	5.1 6.1.4 12.1.2
SC39	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	
SC40	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件	12.1.1
SC41	- 維運人員應提出相關專網設備管理計畫與設備規格書面文件 - 稽核者檢視系統的實體介面的遠端連線機制以及空中介面的連線機制，並確認其安全保護機制，確認其安全保護功能具備完整的操作、監控、警報等機制	6.1.3
SC42	- 稽核者檢視系統在隱私的傳送安全保護機制，與 5G 訊號中 GUTI 與 IMSI 的交互機制，確認其安全機制是否具備明確對應關係	
SC43	- 維運人員應提出設備規格書面文件	12.1.3
System and Information Integrity (SI)		
SC44	- 維運人員應提出設備規格書面文件 - 稽核者檢視系統的更新機制，並對應書面佐證文件確認其軟體與硬體版本的更新及限制符是否合預期	4.1
SC45	- 維運人員應提出設備規格書面文件	

項目代號	檢測/驗證方法	表 1 資安防護評量表對應
	- 稽核者檢視系統的訊息監控機制，確認其系統安全性與 3GPP 之一般性資安確保要求機制是否相符	
SC46	- 維運人員應提出設備規格書面文件 - 稽核者確認其 5G 管理系統的版本管理模式，並檢查確認了其軟體、硬體跟訊息的完整性是否符合預期	4.2

7.5 5G 專網服務管理系統控制項驗證紀錄表

針對 5G 專網服務管理系統進行控制項驗證記錄建議參閱本文件之附錄 A。針對附錄 A 中之欄位，進行如下說明以利評估，參考如表 4：

表 4 附錄 A 表格欄位填寫說明

項目	欄位名稱	說明/備註
1.	項目代號	參考表 2 內之「項目代號」欄位進行填寫
2.	安全領域	參考表 2「項目代號上之分類」進行填寫
3.	NIST SP 800-53 參考對應	參考表 2 內之「NIST SP800-53 參考對應」欄位進行填寫
4.	項目要求	參考表 2 內之「安全控制項目」欄位進行填寫
5.	資安防護評量項目	透過「項目代號」欄位，連結參考表 3 內之「表 1 資安防護評量表對應」欄位進行測試方法設計。若表 3 內之「表 1 資安防護評量表對應」欄位無數值，則可根據場域實際狀況進行測試方法設計
6.	測試方法	根據場域現況及不同的控制項內容進行實際的測試方法設計
7.	測試步驟	根據設計出的測試方法進行逐步測試項展開
8.	預期結果(通過條件)	根據逐步測試展開項，詳列預期產出說明
9.	測試紀錄	紀錄系統輸出
10.	測試結果	通過/不通過
11.	改善建議	如果測試結果為不通過，則需要進行測試步驟的檢視及提出相應的措施

透過控制項驗證及紀錄表實施，業者可評估 5G 專網服務管理系統是否符合「NIST 5G CYBERSECURITY - Preparing a Secure Evolution to 5G」的規範。後續可根據公司資安政

策，定時持續性進行控制項驗證以達到基本資安評估。若業者單位有進行如 ISO27001 導入，也可將紀錄表的紀錄提供成佐證資料進行參考。

附錄 A
(參考)
5G 專網系統安全控制項驗證記錄表-參考範例

表 A.1 安全控制項驗證記錄-參考範例

測試項目	項目代號	安全領域	NIST SP 800-53 參考對應
	SC01	**Access Control (AC)**	AC-3 Access Enforcement
項目要求	電信系統之核心網路(5G Core Network)元件應具備合適的訪問控制策略機制，並於核心網路的管理介面進行實作，僅能執行已經授權的存取，並有效保護訊息跟系統資源，包含訪問控制的策略(policies)、公司帳號群組應具備設置文件、設備帳號應有群組清單、帳號應歸屬分類等。		
資安防護評量項目	11.1.1 檢視存取控制的政策 11.1.2 確認是否有特定維護帳號的登入 LOG		
測試方法	透過 SSH 登入管理介面		
測試步驟	1. 登入管理介面 2. 以指令查詢使用者帳戶清單，並統計使用者數量 3. 以指令查詢登入紀錄，統計登入過的使用者數量，與使用者 Group		
預期結果(通過條件)	1. 登入專網設備之指令介面並以指令查詢之後，應至少可查證存在兩個以上的使用者帳戶 2. 登入專網設備之指令介面並查詢登入紀錄，比對使用者、維運人員有無根據不同的身分 Group 進行登入操作		
測試紀錄	1. 以指令查詢之後，有超過兩個以上的使用者帳戶被統計出來，反映了系統設定確實有根據不同的權限進行設計 2. 查詢登入紀錄之後，反映了使用人員確實有根據不同的 Group / Role 登入的情況		
測試結果			
改善建議			

附錄 B
(參考)
資安防護評估參考工具

表 B.1 資安防護評估參考工具表

檢測項目	參考工具
連接埠掃描	Nmap、Legion、Netcat
使用者鑑別或授權、輸入驗證、邏輯漏洞、連線管理、機敏資訊洩漏、CSRF、Injection 測試	Burp Suite、ZAP
弱點掃描	Nessus、Nexpose、Acunetix、Netspark、Nikto
通行碼破解、協定加密強度測試，通行碼強度分析	Hydra、Ncrack、Burp Suite
封包分析、傳輸加密	Wireshark
傳輸加密、中間人攻擊、連線管理、加密通道鑑別等	Ettercap、SSLstrip
協定、系統弱點滲透測試，遠端指令碼執行	Metasploit Framework

參考資料

(1) National Institute of Standards and Technology (NIST)，SP 1800-33 5G Cybersecurity，2022/04

(2) Cybersecurity and Infrastructure Security Agency (CISA)，Potential Threat Vectors to 5G Infrastructure，2021/05

(3) Cybersecurity and Infrastructure Security Agency (CISA)，5G Security Evaluation Process Investigation，2022/05

(4) TAICS TR-0022，物聯網場域資安防護評估指引 v1.0

(5) TAICS TR-0025，5G Open RAN資安研究報告 v1.0

(6) TAICS TS-0035，5G基地臺資安測試規範 v1.0

(7) 3GPP 33.117，Catalogue of general security assurance requirements

(8) 3GPP 33.501，Security architecture and procedures for 5G System

(9) 3GPP Security Assurance Specification (SCAS) Series (3GPP 33.511, 33.512, …, 33.522)

(10) 3GPP 33.818 Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products

(11) O-RAN，O-RAN Architecture Description v9.00, 2023/03

(12) O-RAN，O-RAN Use Cases Analysis Report v11.00, 2023/03

版本修改紀錄

版本	時間	摘要
v1.0	2023/11/16	出版

地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw